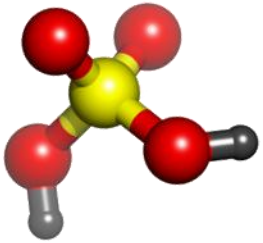


Chemical Storage

SAND No. 2012-5234C, 2010-2279C
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

CSP
CHEMICAL SECURITY
ENGAGEMENT PROGRAM

SAND 2012-5234C

Sandia
National
Laboratories

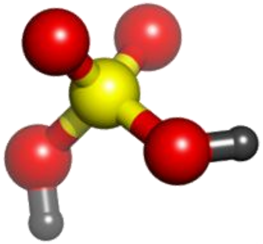
Storing Your Chemicals

- Storage Risk Management
- Storage Facility Design
- General Guidelines
- Reactive Chemicals
- Compressed Gas Cylinders
- Examples
- Access Control

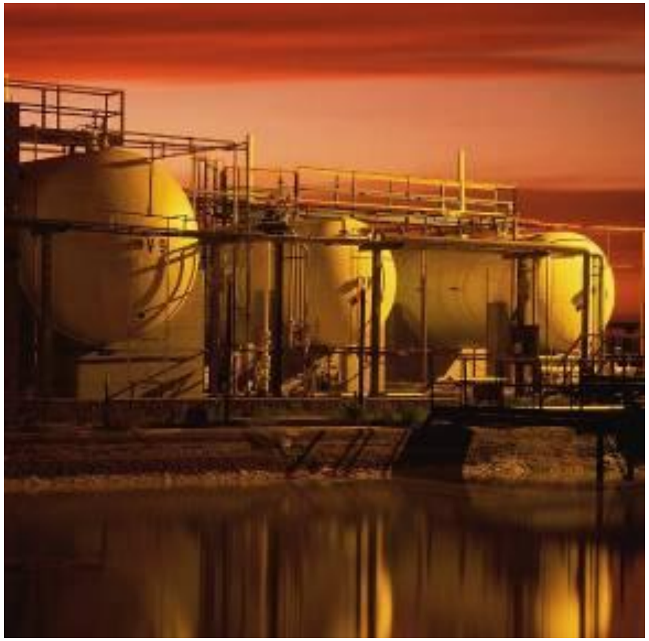
CSP CHEMICAL SECURITY ENGAGEMENT PROGRAM

Chemical SAFETY AND SECURITY TRAINING

Chemical Storage: Risk Management



- What chemicals are needed?
- Where will chemicals be stored?
- What are the hazards associated with chemical storage?
- Have the hazards been evaluated?
- Storage facility design considered?
- What measures can be taken to mitigate risk?

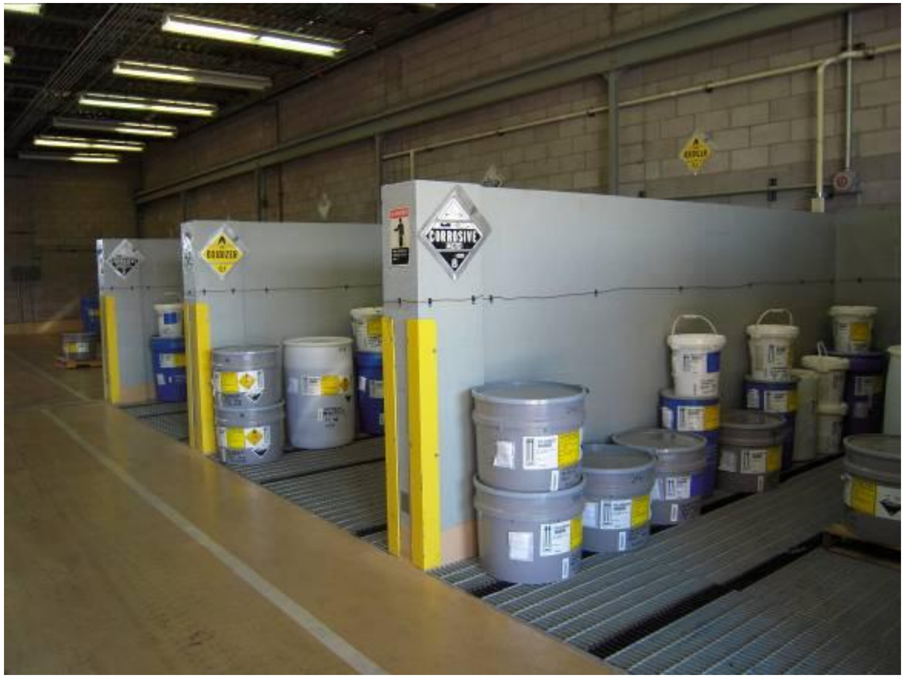


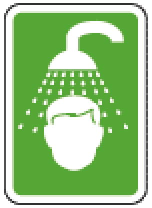
Chemical Storage: Risk Management

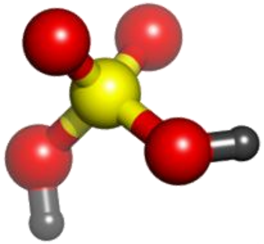
- *Select the type of storage on basis of:*
  - Quantity
  - Concentration
  - Chemical properties
    - State: gas, liquid, or cryogenic
    - Flammability
    - Toxicity
    - Reactivity
  - Storage conditions
    - Temperature and pressure

Storage Facility Design

- Secondary containment for spills or releases
- Fire detection, alarms, and suppression systems
- Safety and emergency response equipment
- Adequate ventilation
  - General ventilation
  - Local exhaust ventilation for transfers
- Access controls
- Alarms/sensors

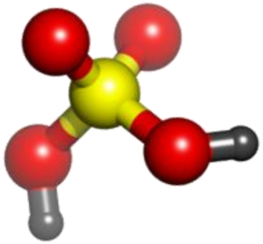






Chemical Storage: General Guidelines

- Separate incompatible chemicals
- Separate flammables and explosives from ignition sources
  - flammable storage cabinets
- Large containers on bottom shelves
- All containers properly labeled and closed

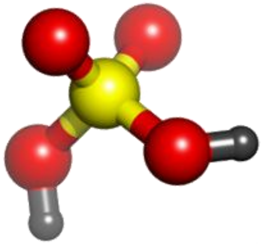


Chemical Storage: General Guidelines

- Wipe-off outside of container before returning to storage area
- Secure Chemicals of Concern
- Use secondary containment
  - Label with compatibility group
- Fasten storage shelves to wall or floor
- Shelves should have a lip and/or rod

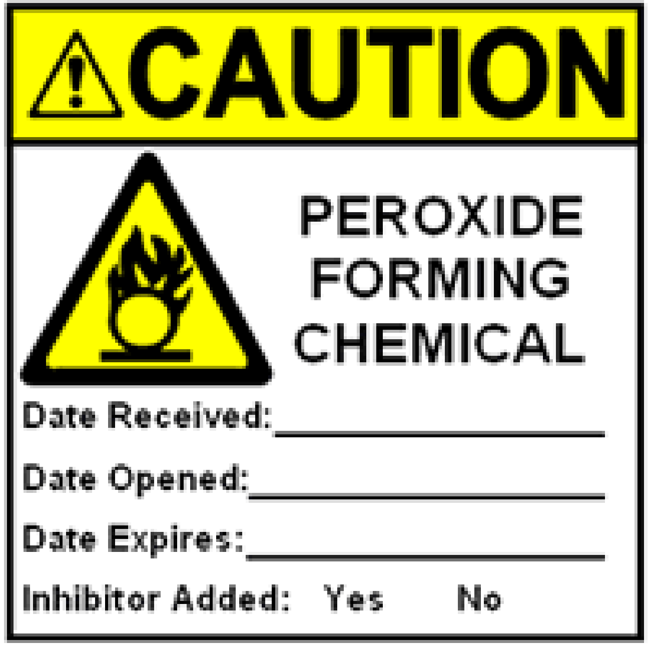
Chemical Storage: General Guidelines

- **Do Not Store Chemicals**
  - On top of cabinets
  - On the floor
  - In hoods
  - Where there are wide variations in temperature, humidity or sunlight
  - In hallways
  - With food



Storage: Reactive Chemicals

- Water reactive, pyrophoric, oxidizers
- Peroxide-forming
  - Ethers, butadiene, tetrahydrofuran
  - Store in tightly closed original container
  - Avoid exposure to light, air, heat
  - Crystals or discoloration? Do not move or open container
  - Test for peroxides before using
    - Especially if distilling/concentrating
  - Know when to dispose
    - Mark when opened
    - Dispose even if unused



⚠CAUTION

PEROXIDE FORMING CHEMICAL

Date Received:_______________

Date Opened:_______________

Date Expires:_______________

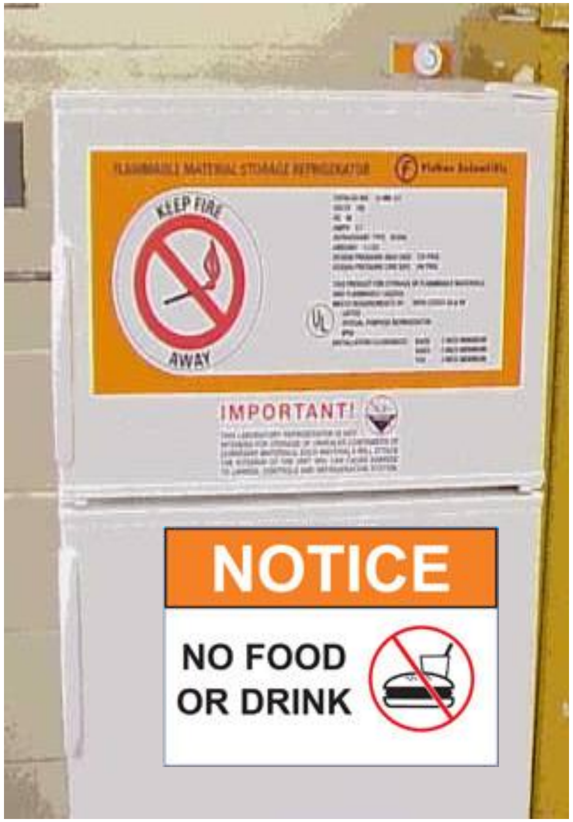
Inhibitor Added: Yes No

Storage: Compressed Gas Cylinders

- Secure (chain/clamp) and separate gas cylinders
- Screw down cylinder caps
- Store in well-ventilated area
- Separate and label empty cylinders
- Separate incompatible gases

Storage: Refrigeration

- Types
  - Ordinary, household refrigerator/freezers
    - Are NOT safe for flammables
  - Flammables-safe refrigerator or freezer
    - May contain flammables, but are NOT safe to be in areas with flammable vapors
  - Explosion-proof storage
- Proper refrigerator/freezer labeling
- Precautions
  - Stable power
  - Not all refrigerants are completely safe
    - Toxicity, flammability, and physical hazards
- Do not store peroxide formers in a refrigerator
- Defrost occasionally to prevent chemicals from becoming trapped in the ice formations

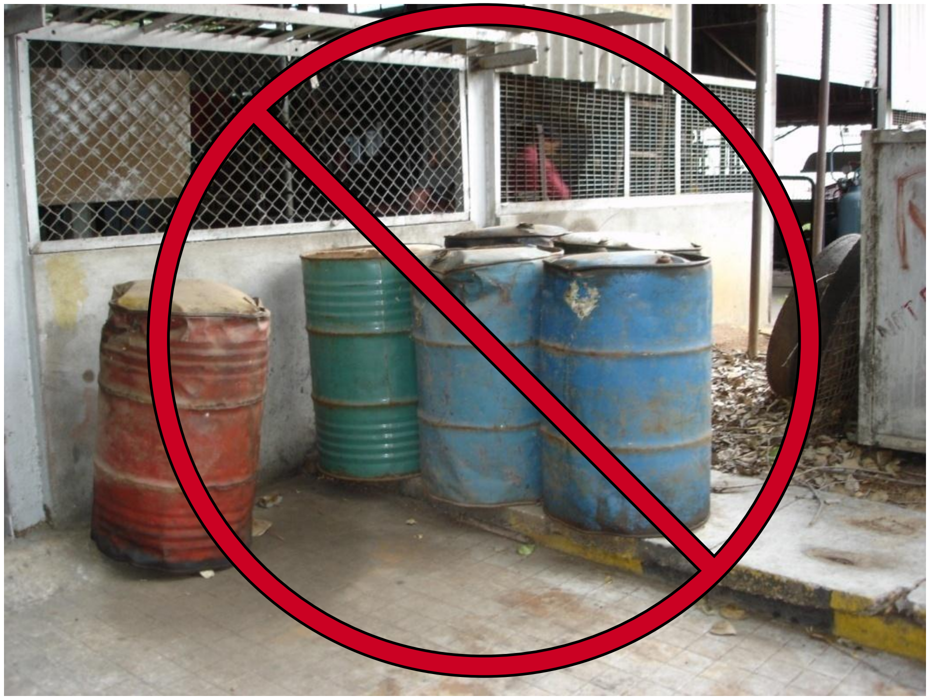


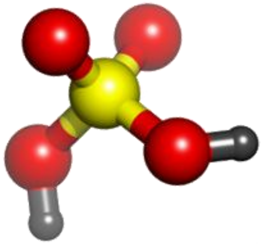
Storage: Drums

- Store drums in areas protected from moisture and high temperatures

- Maintain an inventory of drums
  - Safety data sheets
  - Label drum contents
  - Date waste drums
  - Test for peroxide-forming chemicals regularly

- Inspect drum storage areas for:
  - Corrosion
  - Bulging drums

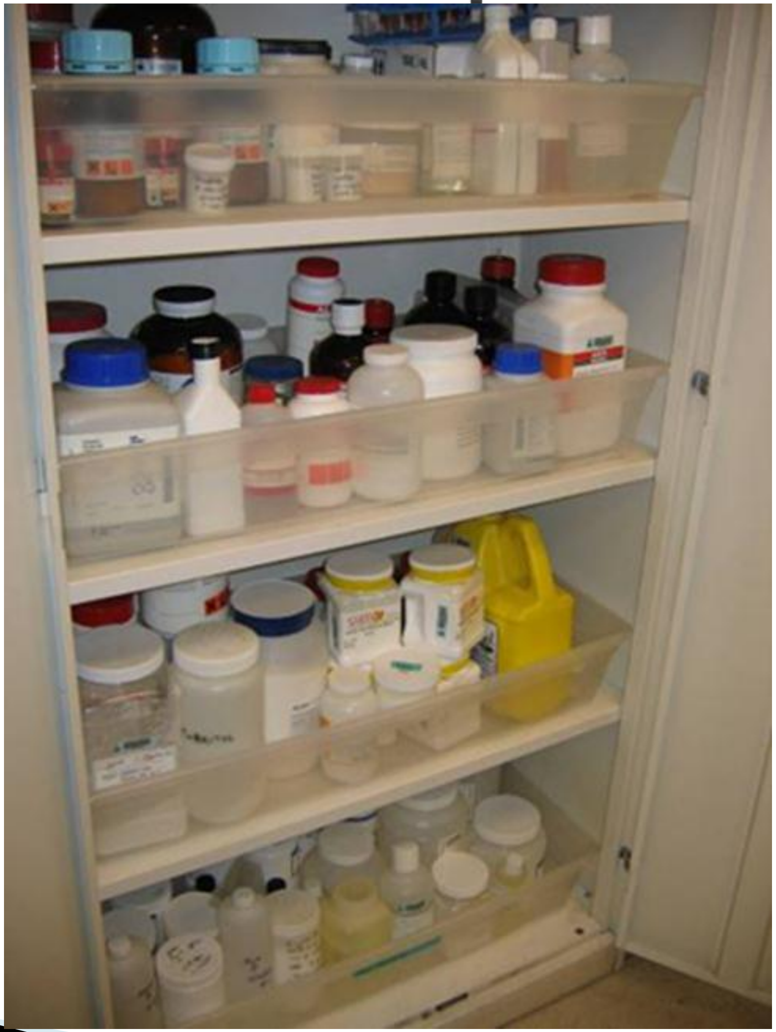


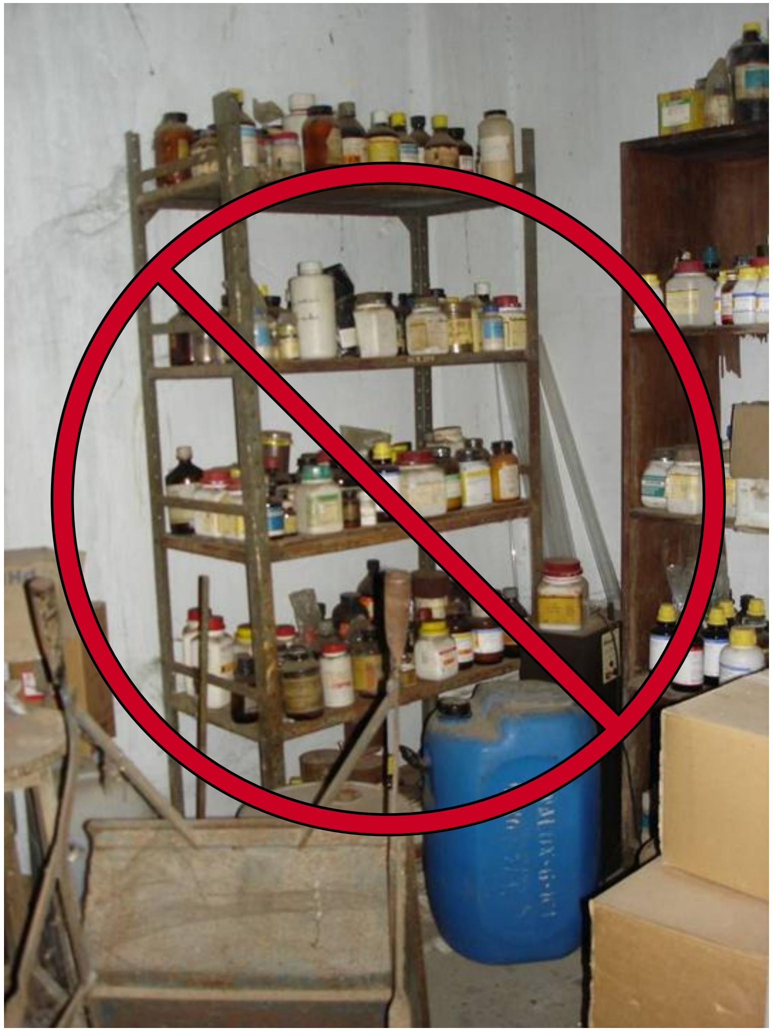


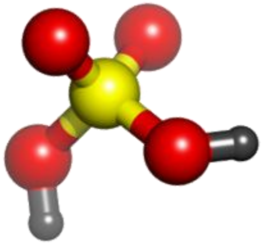
Storage: Access Control

- Access limitations depend on the material or information
  - More control of access if chemicals of concern are present
- Lock areas, rooms, cabinets
  - Control of keys
- Label areas “Authorized Personnel Only”
  - Means of identifying authorized personnel
    - Challenge unfamiliar people in restricted areas
- Authorized personnel
  - Trusted, background check
  - Trained
  - Legitimate need

Storage: Good and Bad Examples







Chemical Storage

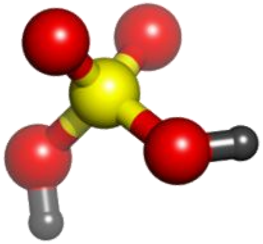
Conclusions

- It is possible to make chemical storage safer and more secure

- Safe and secure chemical storage requires
  - Space
  - Time
  - Training
  - Equipment

- Difficulties may be mitigated by operational controls
  - Substitution
  - Source reduction

- Can get help from an inventory system that tracks hazard classes



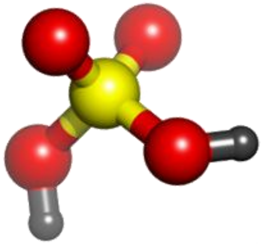
Chemical Transportation Risk Management

SAND No: 2012-2778C
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

CSP
CHEMICAL SECURITY
ENGAGEMENT PROGRAM

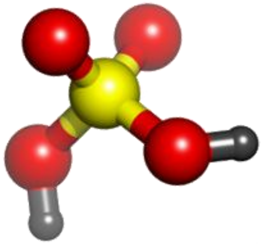
SAND 2012-5234C

Sandia
National
Laboratories



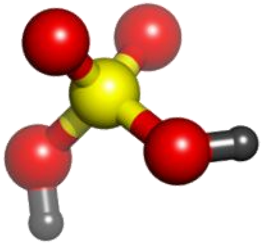
Introduction

- Chemical Transportation
- Case Study Involving the Shipment of Lithium Batteries
- Chemical Transportation Risk Management - Safety
  - Resources to help manage risks
  - Identify, analyze and reduce risks
  - Safety risks
- Chemical Transportation Risk Management - Security
  - Resources and Regulations
  - Identify, analyze and reduce security risks
- Summary



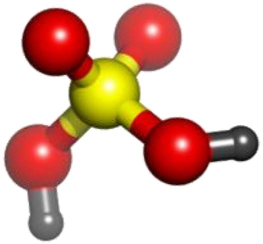
Types of Chemical Transportation

- Chemical transportation:
  - Inside the plant
    - trucks, forklifts, pipelines, etc.
  - Local
    - Vehicles - company owned, contract services
    - pipelines
  - In-country
    - Similar to local
    - Trains
    - Ships
    - Air transport
  - International transport
    - Trucks (company owned or contract services), pipelines
    - Trains
    - Ships
    - Air transport



Chemical Transportation

- It is an essential element in the chemical supply chain and
- Globalization has resulted in:
  - Increased volume
  - Increased speed
  - Strain on transportation infrastructure



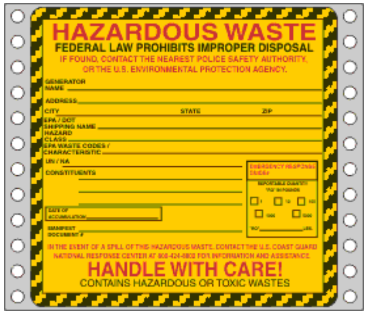
Chemical Transportation Safety Risks

- Transporting hazardous chemicals and hazardous waste

  Risks to *people, facilities, communities* and the *environment*

- Transport vehicle may carry both people and product

- Transport companies may outsource and consolidate hazardous materials
  - Package incompatible materials
  - Insecure packaging & improper labeling



HAZARDOUS WASTE

FEDERAL LAW PROHIBITS IMPROPER DISPOSAL

IF FOUND, CONTACT THE NEAREST POLICE SAFETY AUTHORITY, OR THE U.S. ENVIRONMENTAL PROTECTION AGENCY.

GENERATOR NAME ____

ADDRESS ____

CITY ____ STATE ____ ZIP ____

EPA / DOT SHIPPING NAME ____

HAZARD CLASS ____

EPA WASTE CODES / CHARACTERISTIC ____

UN / NA ____

CONSTITUENTS ____

DATE OF ACCUMULATION ____

MANIFEST DOCUMENT # ____

EMERGENCY RESPONSE GUIDE#

REPORTABLE QUANTITY "RQ" IN POUNDS

□ 1 □ 10 □ 100

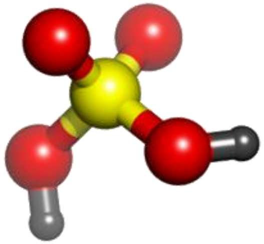
□ 1000 □ 5000

"RQ" ____ LBS.

IN THE EVENT OF A SPILL OF THIS HAZARDOUS WASTE, CONTACT THE U.S. COAST GUARD NATIONAL RESPONSE CENTER AT 800-424-8802 FOR INFORMATION AND ASSISTANCE.

HANDLE WITH CARE!

CONTAINS HAZARDOUS OR TOXIC WASTES



Current Complexity in Chemical Transportation Increases Risk

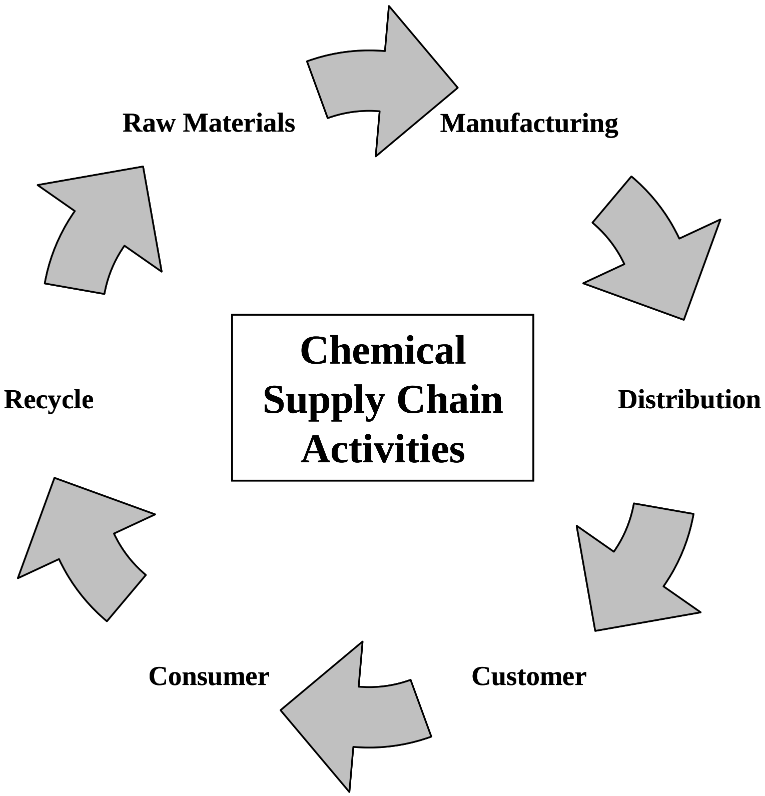
- Thousands of regulated hazardous materials
- Differences in regulations by country
- Use of different hazard classes
- Different modes of transportation
  - Road, rail, air, marine, pipeline
- Multiple packaging types

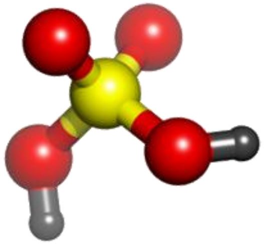
Transportation Risk Management

Due to the complexity of many supply chains, transportation risk management is a shared responsibility.

Roles and responsibilities may differ for each stakeholder.

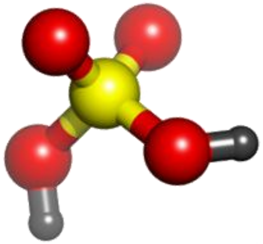
Individual activities and actions can impact the risk to the overall *chemical supply chain.*





A Case Study Involving Lithium Batteries and Improper Packaging

Accident No. DCA04MZ001U.S. National Transportation Safety Board. http://www.ntsb.gov/



A Case Study Involving Lithium Batteries and Improper Packaging

Transportation mode: Air

Date: 7 Aug. 2004

Hazardous Material: Lithium-ion batteries

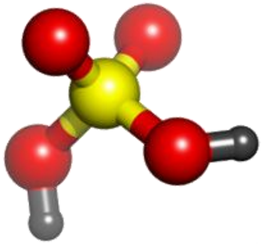
Type of accident: Cargo fire at the terminal

Carrier: Air freight line (non-passenger carrier)

Result: Damage to cargo unit load device ~$20,000 USD.

No injuries.

Accident No. DCA04MZ001U.S. National Transportation Safety Board. http://www.ntsb.gov/

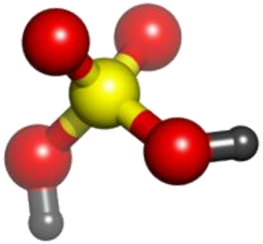


A Case Study Involving Lithium Batteries and Improper Packaging…

Background Information:

- Lithium batteries are described as Class 9 goods [miscellaneous dangerous goods – international term is hazardous materials].
- This was a prototype battery pack manufactured by a US firm.
- Battery pack was to be shipped to France for electric car research.
- Because it was a prototype battery pack special approval was required for this shipment.

U.S. National Transportation Safety Board.
http://www.ntsb.gov/



A Case Study Involving Lithium Batteries and Improper Packaging

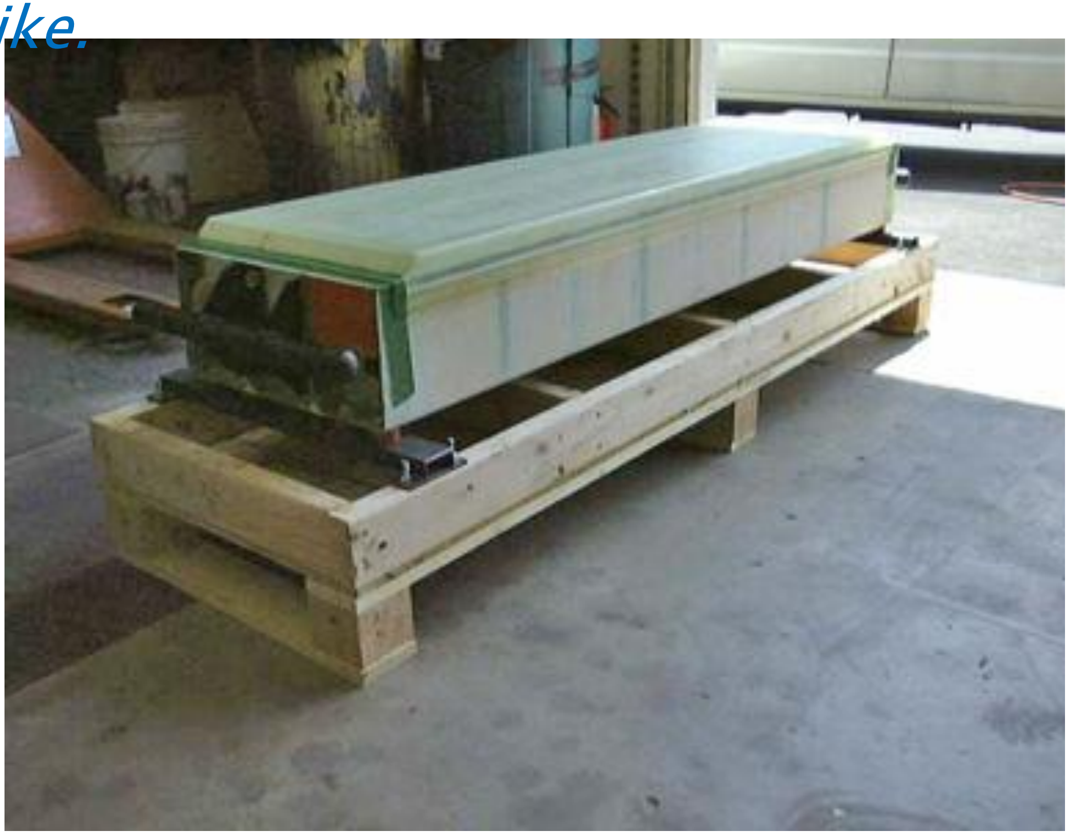
Shipping Requirements as specified by the US Department of Transportation –

- Battery pack
  - Size - 157 x 43 x 23 cm
  - Weight = 159 Kg
- Package specifications –
  - Insulating fiber glass case
  - Inside a wooden box
  - Fiberglass case bolted to the wooden box
  - Total weight = 240 Kg

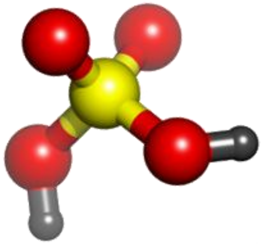
U.S. National Transportation Safety Board.
http://www.ntsb.gov/

A Case Study Involving Lithium Batteries and Improper Packaging…

This is what the packaging was supposed to look like.



U.S. National Transportation Safety Board. http://www.ntsb.gov/



A Case Study Involving Lithium Batteries and Improper Packaging…

How did the company prepare the lithium battery pack for packaging?

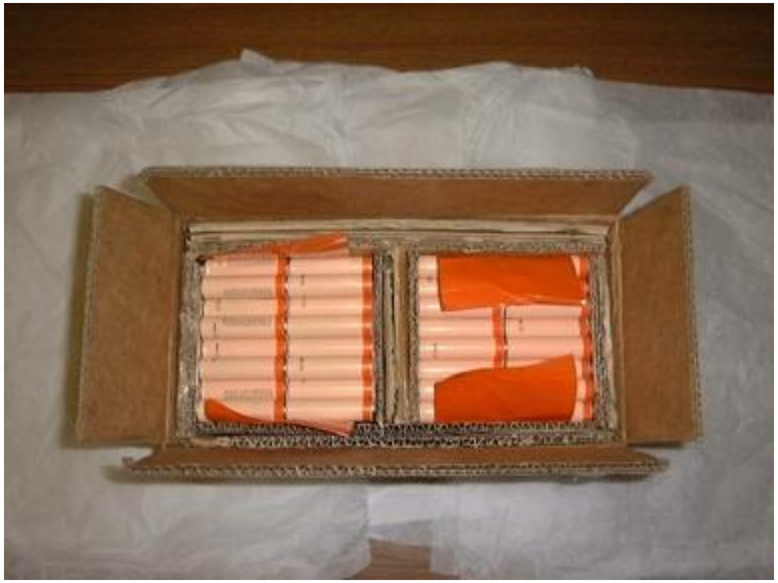
- Type of Package –
  - Cardboard box

- The package contained –
  - Battery pack with exposed terminals
  - Metal wrenches with a plastic bag of nuts and bolts.

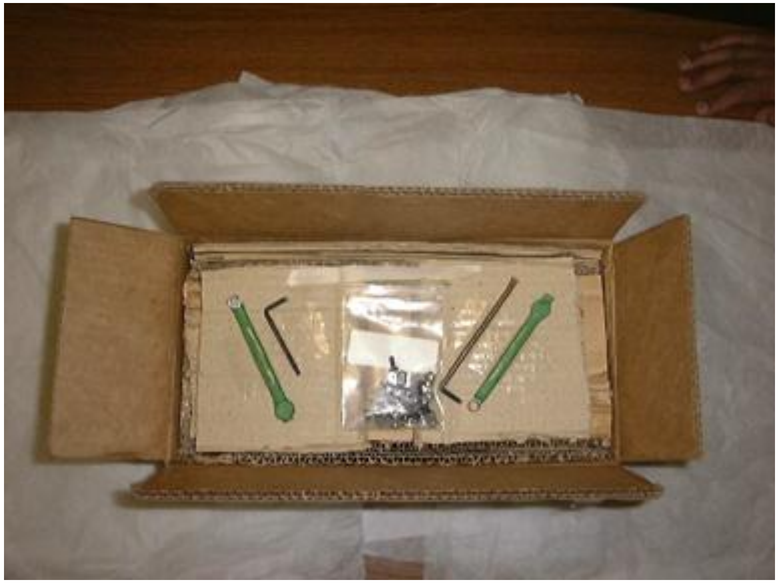
U.S. National Transportation Safety Board.
http://www.ntsb.gov/

A Case Study Involving Lithium Batteries and Improper Packaging…

This is how the battery packs were packaged.



Cardboard box with battery packs



Metal tools inside the same box.

U.S. National Transportation Safety Board.
http://www.ntsb.gov/

A Case Study Involving Lithium Batteries and Improper Packaging…

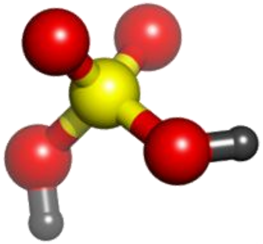
What Happened?

- It was determined that the metal tools shifted during transportation and short circuited the positive and negative terminals of the battery pack causing localized heating.
- This heating caused the packaging to burn and ruptured of some of the other lithium ion battery cells.

U.S. National Transportation Safety Board.
http://www.ntsb.gov/

A Case Study Involving Lithium Batteries and Improper Packaging…

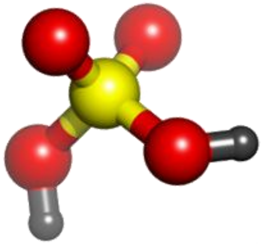
Why did this accident happen?



A Case Study Involving Lithium Batteries and Improper Packaging…

There were guidelines detailing the proper packaging of the lithium-ion batteries.

These guidelines were not followed.

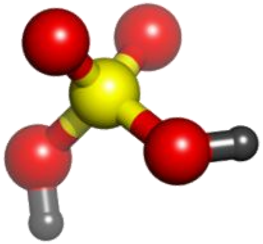


A Case Study Involving Lithium Batteries and Improper Packaging…

What could have been the outcome?

This fire could have occurred during the flight, resulting in the loss of the airplane and possibly the loss of life.

The freight box containing the battery pack was being loaded into the airplane when the worker smelled smoke.



Transportation Risk Management

Center for Chemical Process Safety (CCPS) Risk Management Publication

CCPS (2008). Guidelines for Chemical Transportation Safety, Security, and Risk Management

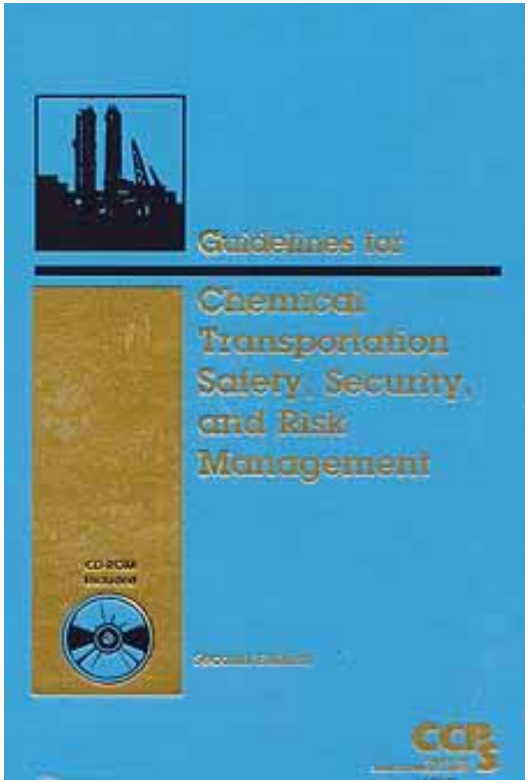
Covers transportation safety, security and risk management

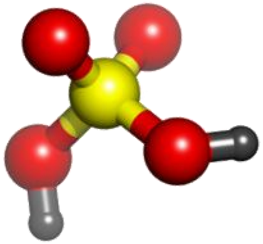
Provides tools and methods to assist transportation professionals and other stakeholders

Presents a comprehensive framework for managing transportation risks

Introduces practical techniques for screening, identifying, and managing higher-level risks

Emphasizes the need to balance safety with security

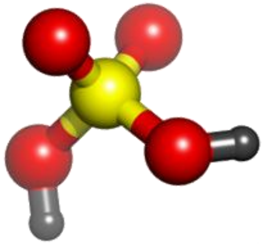

Guidelines for
Chemical Transportation Safety, Security, and Risk Management
CD-ROM Included
Second Edition
CCPS



Transportation Risk Management

To help calculate risks –

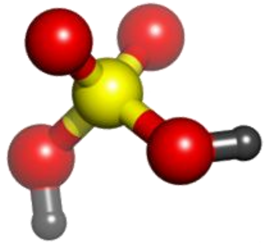
- *CCPS Guidelines* gives estimates for the likelihood of incidents involving:
  - Pipelines
  - Rail
  - Trucks
  - Barges
  - Ocean-going vessels
  - Intermodal transport



CCPS Transportation Risk Management (TRM)

The CCPS TRM process includes the following elements:

- Primary Management System
- Identification and prioritization of hazards
- Risk Analysis
- Risk Reduction
- Program Sustainability



Transportation Risk Management
Primary Management System

Primary Management Systems

Management systems should adhere to regulations and accepted international transportation standards.

- UN Model Regulations

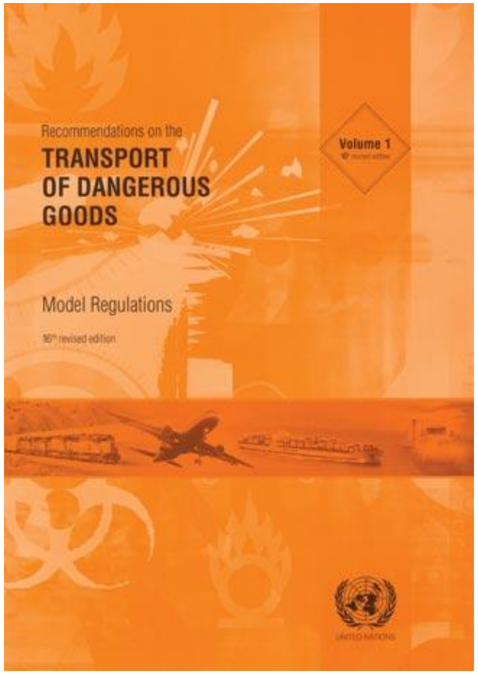
  http://www.unece.org/trans/danger/publi/unrec/12_e.html

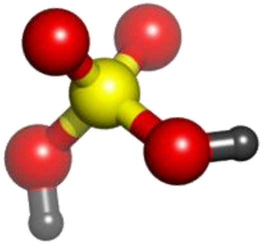
- International Maritime Organization (IMDG Code)

  http://www.imdgsupport.com/

- International Air Transport Association (IATA)

  Dangerous Goods Regulation, 52nd Ed.



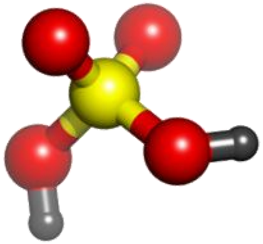


Transportation Risk Management Primary Management System

A Primary Management System Should Also Include:

- Management Commitment

  “Risk Reduction Culture”
- Policies, procedures & practices
- Emergency preparedness & response procedures
- Incident reporting system
- Management of change
- Periodic auditing of the system



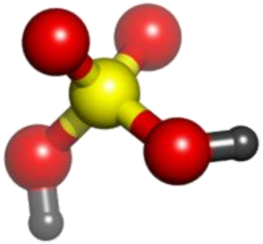
Transportation Risk Management Model

Risk = f(scenario, consequence, likelihood)

Transportation risk management follows a general risk management model -

1. **Identification and Prioritization:** screen to identify and escalate issues/scenarios for more detailed risk analysis.
2. **Analysis:** the process of evaluating and estimating the overall level of risk associated with the selected scenarios.
3. **Evaluation:** compare the results against evaluation criteria used for making decisions to set the level of risk mitigation.
4. **Reduce:** develop, compare and select ways to reduce the risks to a target level if needed or as needed.

CCPS Guidelines for Chemical Transportation Safety, Security, and Risk Management



Transportation Risk Management
Identify Risks

What are the hazardous materials that will be transported?

- What are the physical and chemical properties of the materials?
  - Flammable, toxic, corrosive, reactive?
  - Gas or liquid?
- (How are they packaged?)

Photos: U.S. Department of Transportation

Transportation Risk Management
Analyze Risks

External (Accidents)

- Collisions-road, rail
- Cargo shift-road, air
- Derailment-rail
- Crash-air
- External impact-pipeline

Internal Events

- Release or spill that is not due to an external impact
- Example: equipment or containment failure

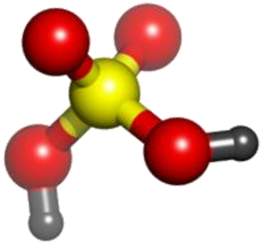
Photos: US National Transportation Safety Board

Transportation Risk Management
Analyze Risks

Potential Causes of Incidents

- Human factors
- Equipment defects
  - Corrosion
  - Overpressure
- Overfilling
- Improper packaging
- Vehicle impact
- Transportation infrastructure

Photo: US National Transportation Safety Board



Transportation Risk Management

Analyze Risks

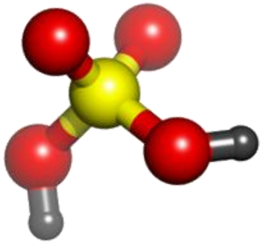
Risk = f(scenario, consequence, likelihood)

Consequence

- Fatalities/injuries
- Property damage
- Environmental damage
- Business impact/fines
- Negative media
- Distribution system disrupted

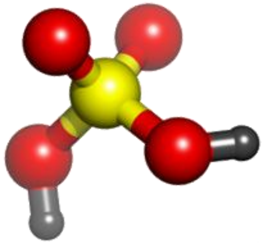
Likelihood

- Expected probability and frequency



Transportation Risk Management
Evaluate Risks

- After analyzing the risks with respect to possible
  - Scenarios,
  - Consequences and
  - Likelihood.
- Compare the results against evaluation criteria that was used and
- Make decisions to set the level of risk mitigation.

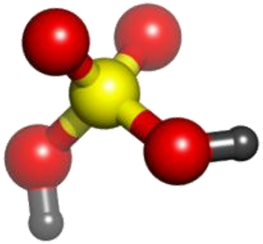


Transportation Risk Management

Risk Reduction

Address highest priority safety hazards first by:

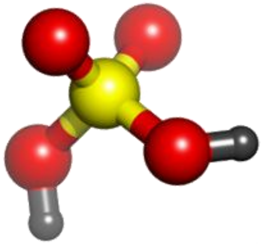
- Written procedures
- Personnel training
- Hazard communication
- Packaging
- Spill containment
- Equipment inspection
- Personnel protection (PPE)
- Emergency response and reporting



Transportation Risk Management
Risk Reduction

Written procedures –

Written procedures outlining different steps and procedures associated with shipping and receiving chemicals for your company.



Transportation Risk Management

Risk Reduction

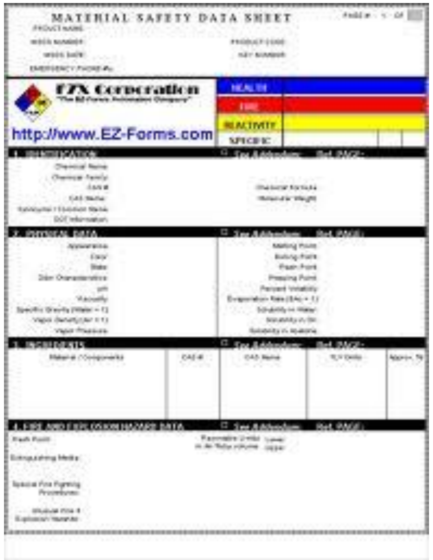
Personnel Training –

- Train personnel on the handling, packaging, shipping and receiving of chemicals.
- They need to know local transportation as well as international regulations for the shipment of hazardous chemicals.
- Make sure that more than one person has the training.
- Make sure training is up-to-date.

Transportation Risk Management
Risk Reduction

Hazard Communication

- Safety data sheets
- Shipping papers
- Labeling
- Placards (information signs)


MATERIAL SAFETY DATA SHEET

PRODUCT NAME

MSDS NUMBER — PRODUCT CODE

MSDS DATE — KEY NUMBER

EMERGENCY PHONE #s

EZX Corporation
"The EZ-Forms Information Company"
http://www.EZ-Forms.com

HEALTH
FIRE
REACTIVITY
SPECIFIC

1. IDENTIFICATION — □ See Addendum — Ref. PAGE:

Chemical Name
Chemical Family
CAS #
CAS Name
Synonyms / Common Name
DOT Information
Chemical Formula
Molecular Weight

2. PHYSICAL DATA — □ See Addendum — Ref. PAGE:

Appearance
Color
State
Odor Characteristics
pH
Viscosity
Specific Gravity (Water = 1)
Vapor Density (Air = 1)
Vapor Pressure
Melting Point
Boiling Point
Flash Point
Freezing Point
Percent Volatility
Evaporation Rate (BAc = 1)
Solubility in Water
Solubility in Oil
Solubility in Acetone

3. INGREDIENTS — □ See Addendum — Ref. PAGE:

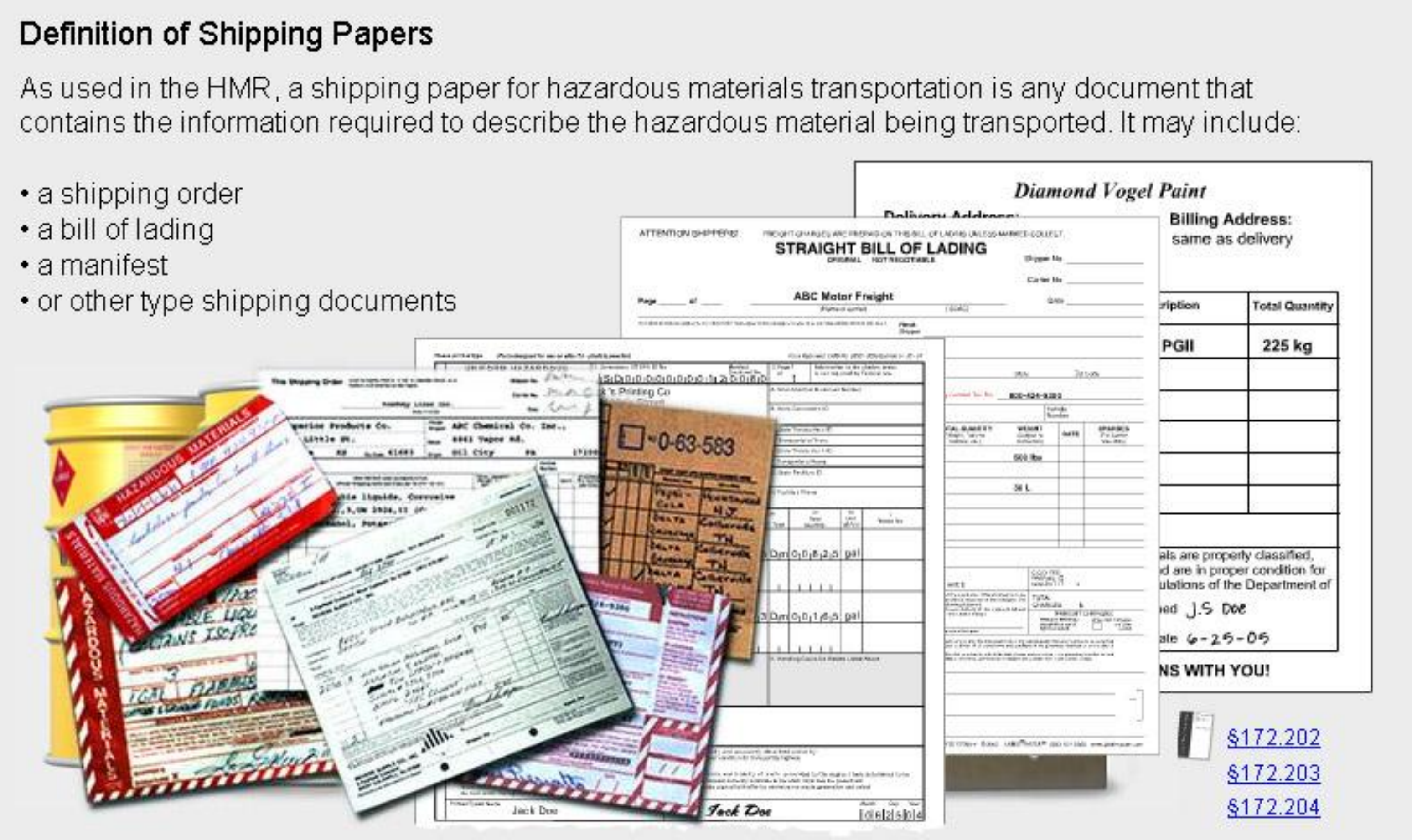
Material / Components	CAS #	CAS Name	TLV Units	Approx. %

4. FIRE AND EXPLOSION HAZARD DATA — □ See Addendum — Ref. PAGE:

Flash Point
Flammable Limits in Air % by volume — Lower — Upper
Extinguishing Media
Special Fire Fighting Procedures
Unusual Fire & Explosion Hazards

Transportation Risk Management

Risk Reduction



Definition of Shipping Papers

As used in the HMR, a shipping paper for hazardous materials transportation is any document that contains the information required to describe the hazardous material being transported. It may include:

- a shipping order
- a bill of lading
- a manifest
- or other type shipping documents

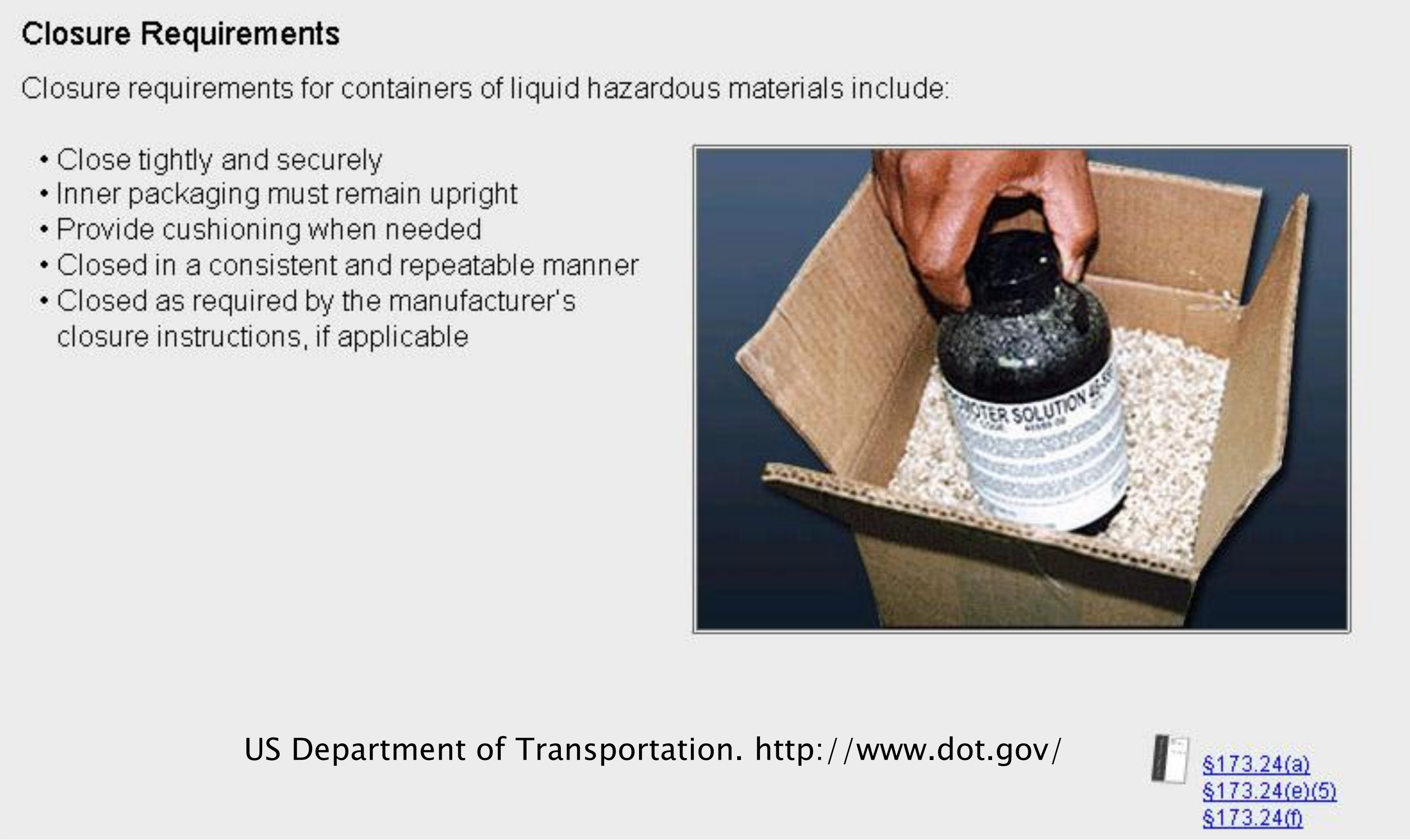
§172.202

§172.203

§172.204

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management
Risk Reduction



Closure Requirements

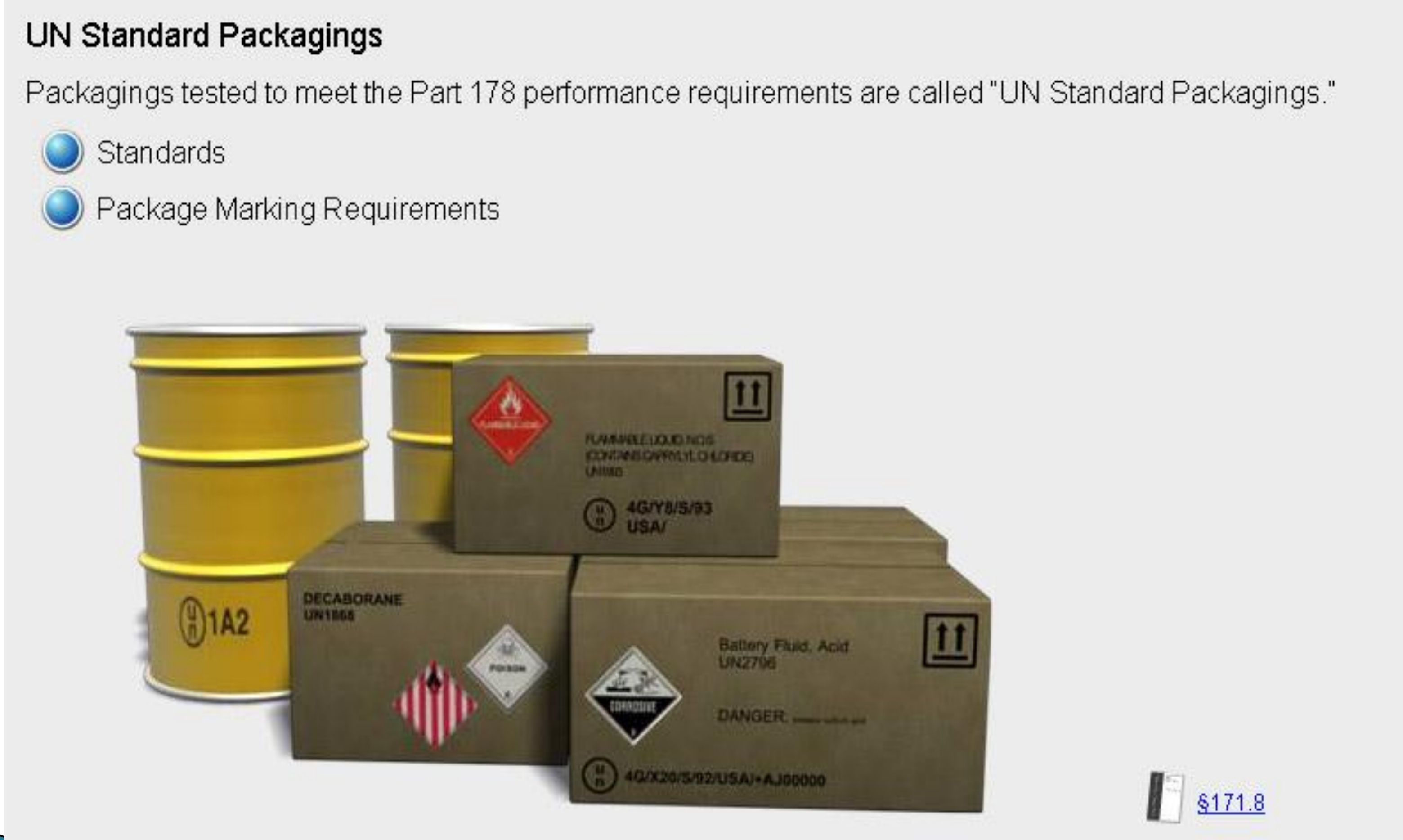
Closure requirements for containers of liquid hazardous materials include:

- Close tightly and securely
- Inner packaging must remain upright
- Provide cushioning when needed
- Closed in a consistent and repeatable manner
- Closed as required by the manufacturer's closure instructions, if applicable

§173.24(a)
§173.24(e)(5)
§173.24(f)

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management
Risk Reduction



UN Standard Packagings

Packagings tested to meet the Part 178 performance requirements are called "UN Standard Packagings."

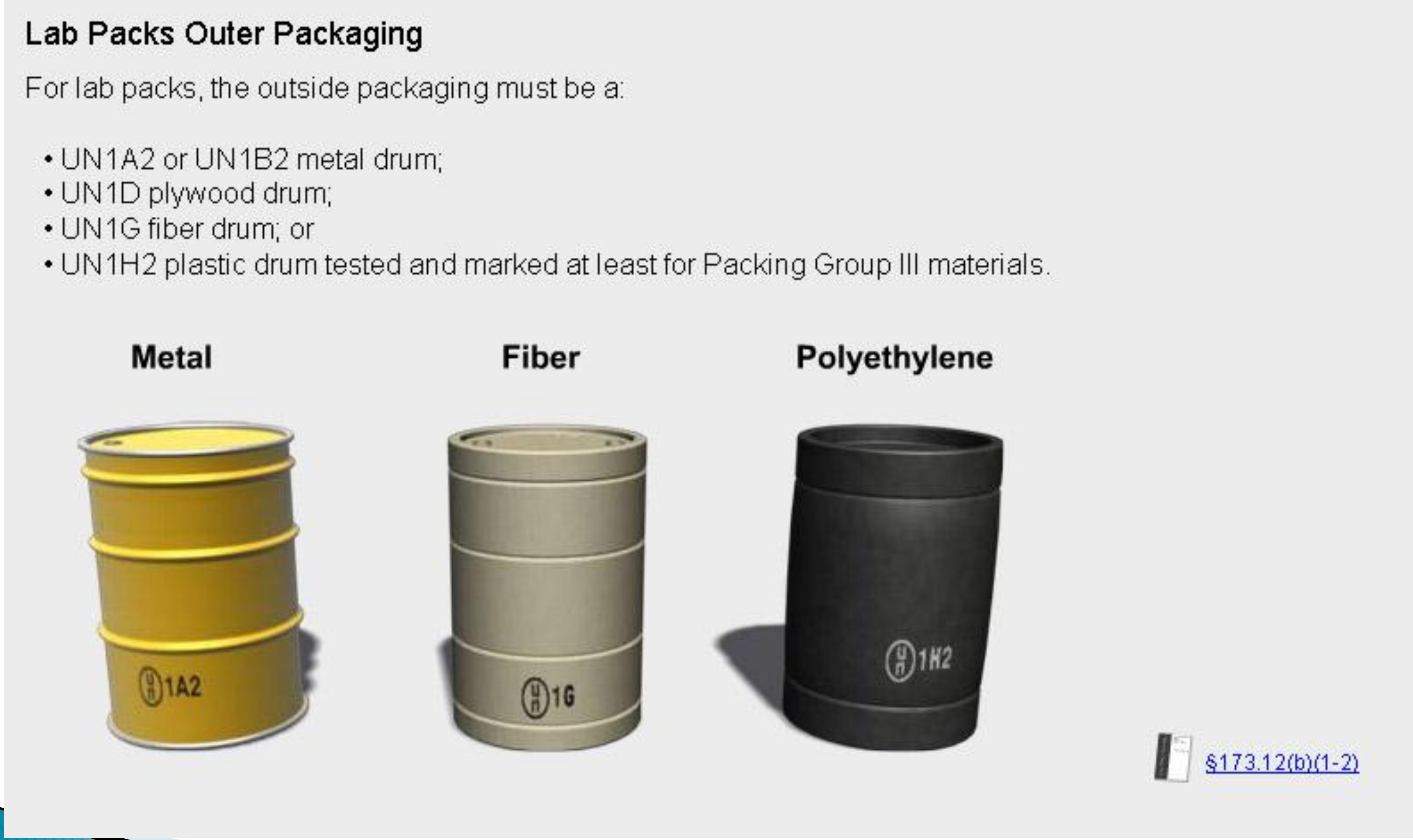
- Standards
- Package Marking Requirements

§171.8

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management

Risk Reduction



Lab Packs Outer Packaging

For lab packs, the outside packaging must be a:

- UN1A2 or UN1B2 metal drum;
- UN1D plywood drum;
- UN1G fiber drum; or
- UN1H2 plastic drum tested and marked at least for Packing Group III materials.

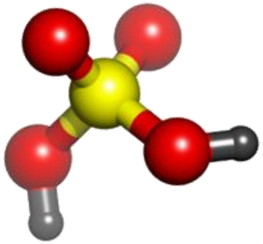
Metal

Fiber

Polyethylene

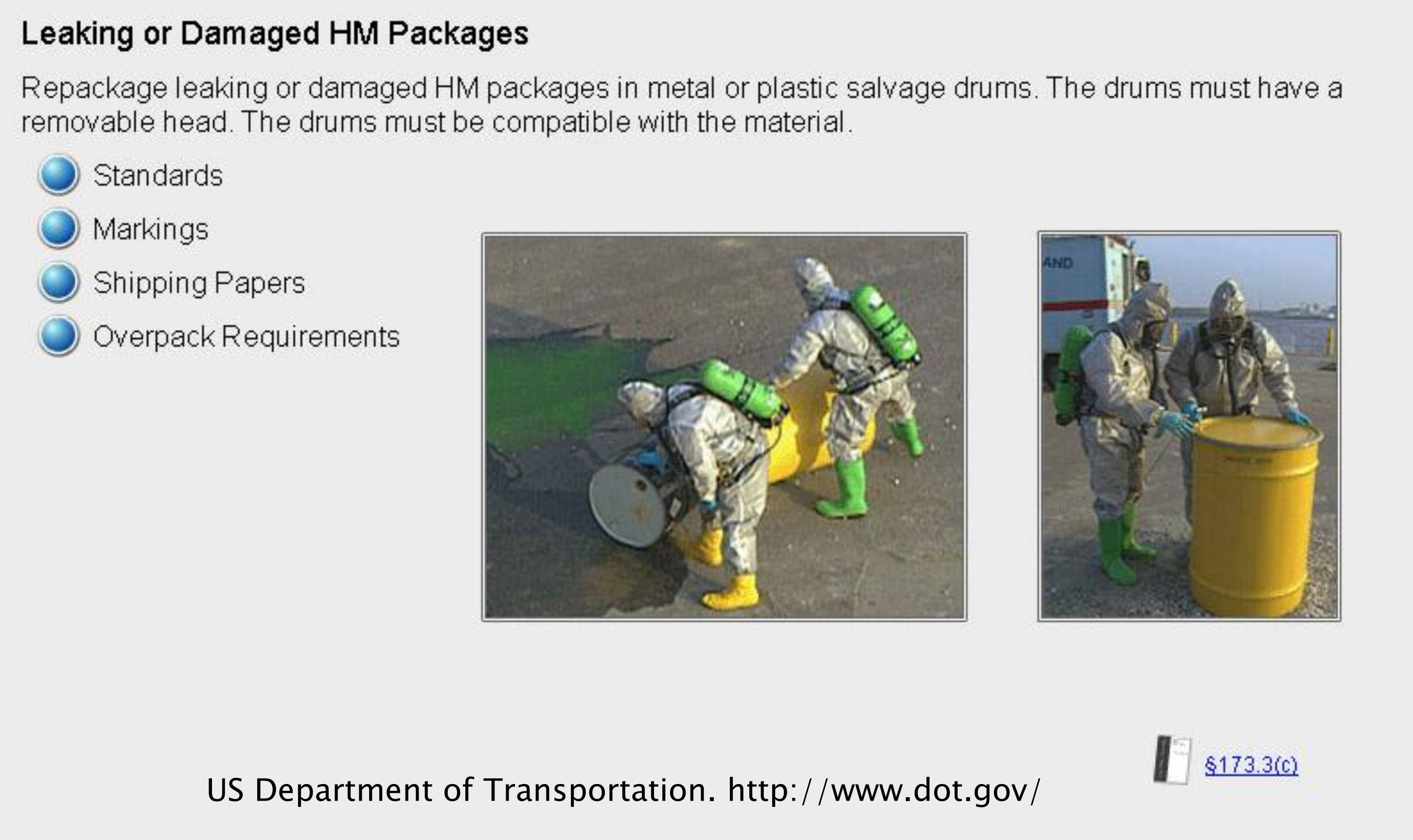
§173.12(b)(1-2)

US Department of Transportation. http://www.dot.gov/



Transportation Risk Management

Risk Reduction



Leaking or Damaged HM Packages

Repackage leaking or damaged HM packages in metal or plastic salvage drums. The drums must have a removable head. The drums must be compatible with the material.

- Standards
- Markings
- Shipping Papers
- Overpack Requirements

§173.3(c)

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management
Risk Reduction

Emergency Response Guidebook (ERG)

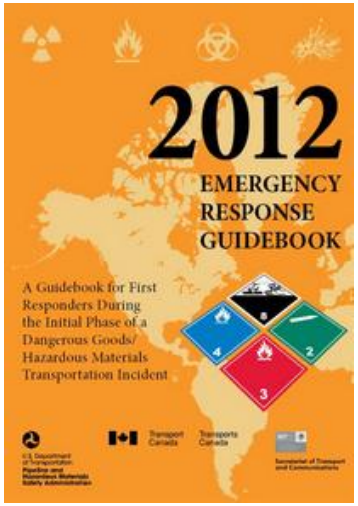
- Interactive internet version:

  http://wwwapps.tc.gc.ca/saf-sec-sur/3/erg-gmu/erg/ergmenu.aspx

- Developed jointly by:

  US DOT, Transport Canada, Secretariat of Communications and Transportation Mexico

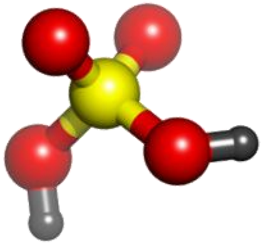
- For first responders to transportation incident
- Guide to quickly identify material classification
- Protect initial responders and public



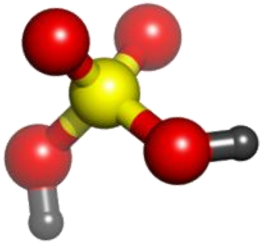
2012

EMERGENCY
RESPONSE
GUIDEBOOK

A Guidebook for First
Responders During
the Initial Phase of a
Dangerous Goods/
Hazardous Materials
Transportation Incident



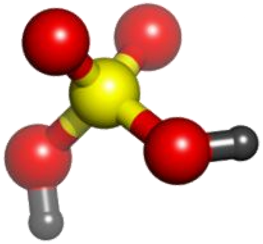
Chemical Transportation Security Risks



Chemical Transportation Security Risks

- In-plant threat
  - Sabotage shipments
  - Intentional release
  - Theft
- In-transit threats
  - Hijacking
  - Theft of materials
  - Sabotage
- Attacks on pipelines

http://www.phmsa.dot.gov/hazmat/security



Transportation Risk Management
Security Risks

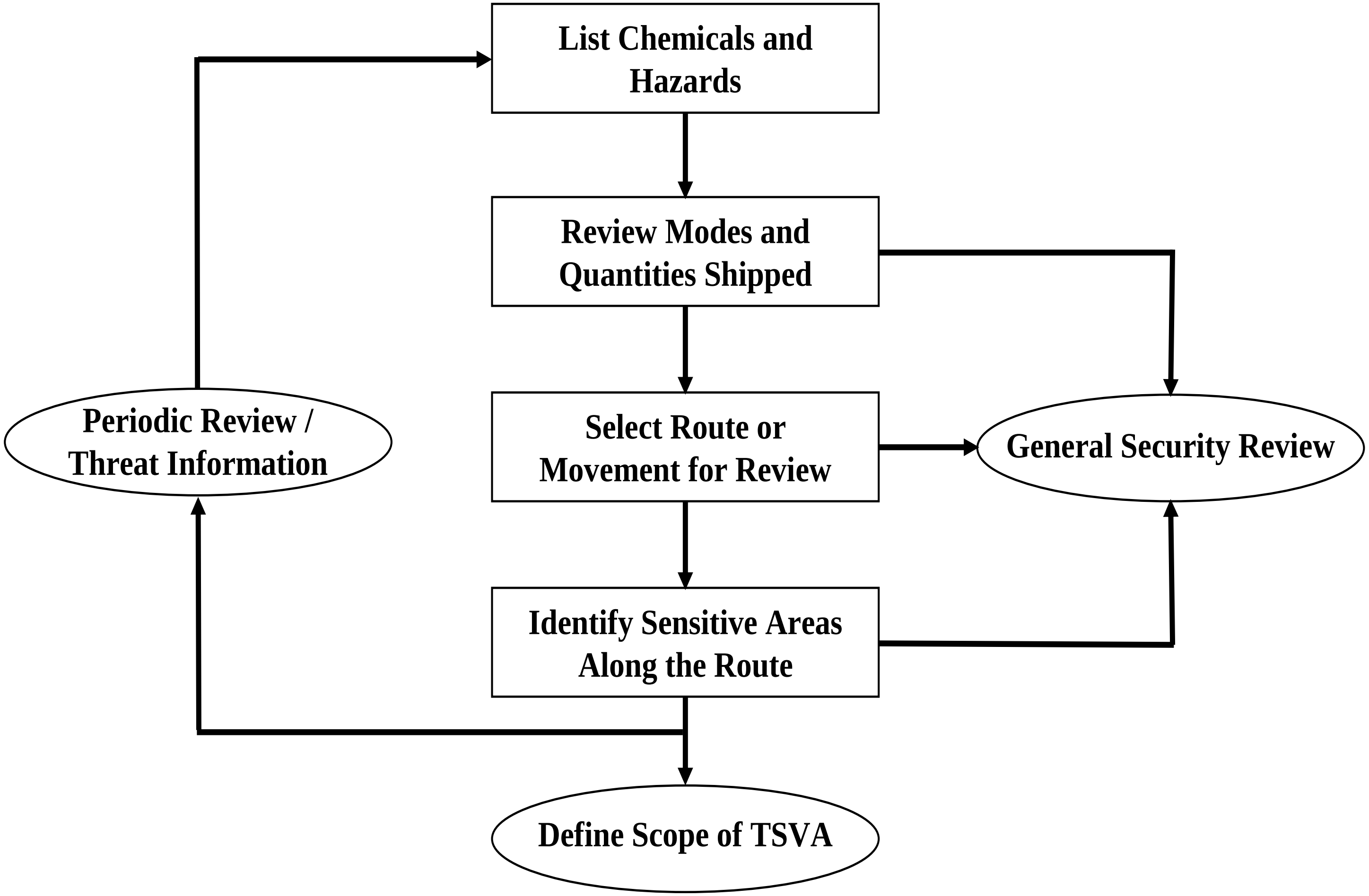
Security Risk = *f*(consequence, vulnerability, threat)

Is similar to safety risks

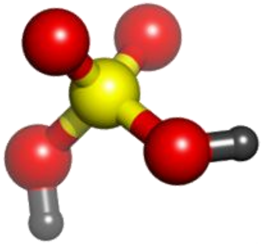
Safety Risk = f(scenario, consequence, likelihood)

- For security risks the initiating event is a direct attack.
- The magnitude of the incident could be greater.
  - Larger releases of hazardous material are possible,
  - Populations would be most likely the target.

Transportation Security Vulnerability Analysis


List Chemicals and Hazards
Review Modes and Quantities Shipped
Select Route or Movement for Review
Identify Sensitive Areas Along the Route
Define Scope of TSVA
Periodic Review / Threat Information
General Security Review

CCPS (2008). Guidelines for Chemical Transportation Safety, Security, and Risk Management



Transportation Security Risk Management Risk Reduction

Plant Security

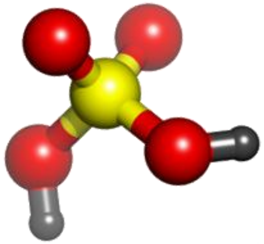
- Include internal transfers in plant security plan
- Limit access to facilities and shipping information
- Secure transportation equipment
- Keep an inventory of hazardous materials
  - Use tamper resistant seals
- Personnel Security
  - Background checks
  - Identification cards or badges

Transportation Security Risk Management
Risk Reduction

In transit security threats

- Vehicle travels on unprotected public roads, rail or sea
- Surroundings are constantly changing
- Sabotage or theft is not detected until in progress
- One person responsible for transport
- Typically there are no security personnel accompanying shipment

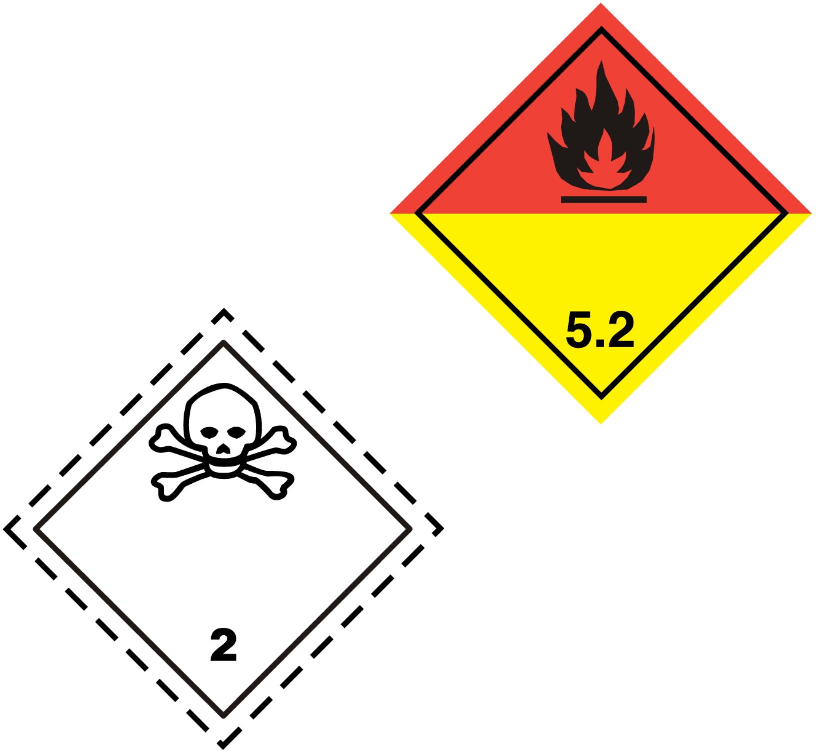
Photo: U. S. Transportation Security Administration



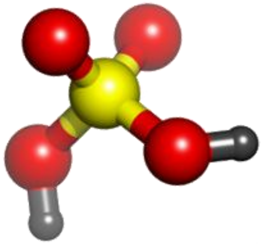
Transportation Security Risk Management
Risk Reduction

Potentially sensitive materials that are shipped by highway

- Depends on quantity and packaging
- ~ ≥ 3000 liters in single container
  - Explosives
  - Flammable Gases
  - Anhydrous Ammonia
  - Toxic Gases
  - Flammable Liquids & Solids
  - Oxidizers
  - Water reactive
  - Corrosives
  - Radioactive, infectious substances



Credit: US TSA Highway Security Sensitive Materials



Transportation Security Risk Management
Risk Reduction

High risk shipments require *high-level* controls:

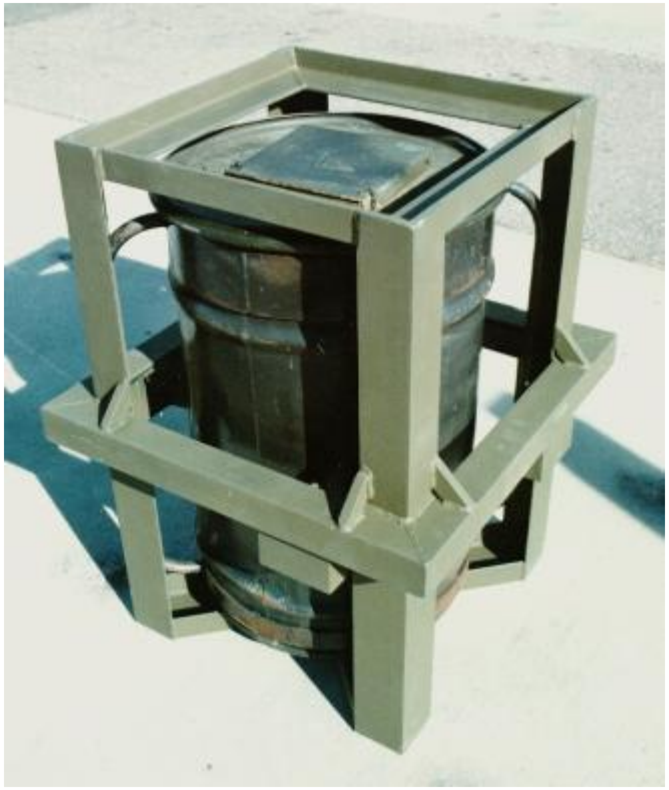
Increase possibility of detecting an attack

- Provide for additional security personnel
- Alarm the shipment
- Use communication systems

Transportation Security Risk Management Risk Reduction

Increase the possibility of delaying an attack

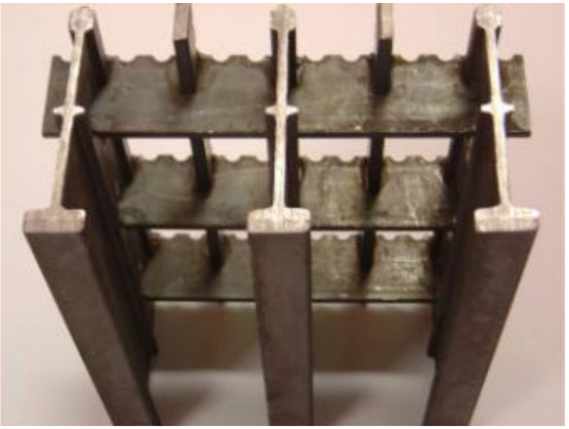
- Cargo secured to vehicle
- Immobilize vehicle
- Hazardous material in vault
- Locks, barriers, entanglements



Drum Cage

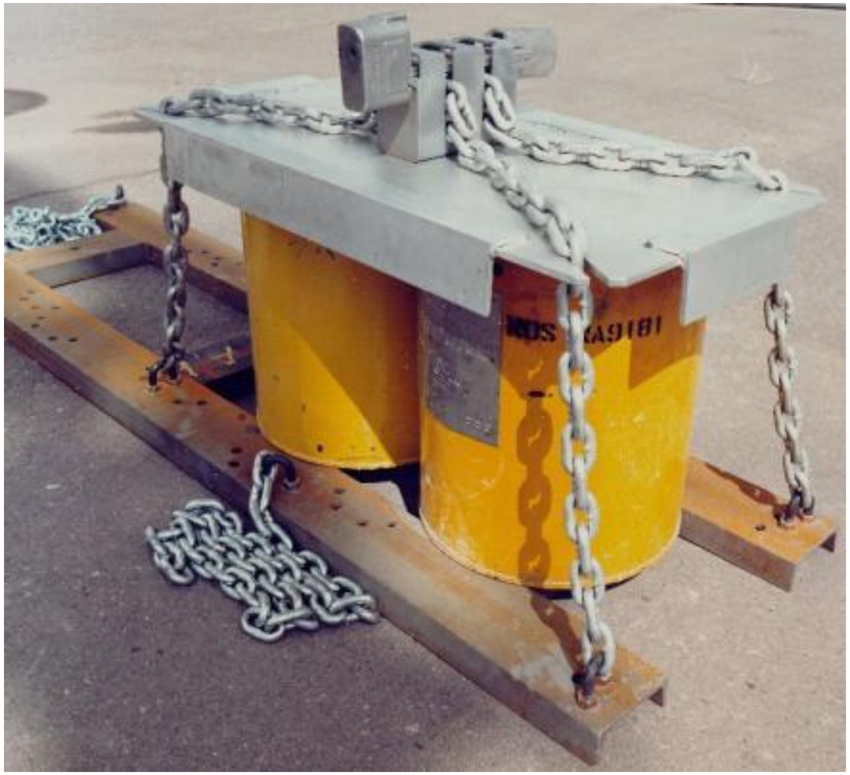
Photo credit: DOE NNSA Presentation, October 17-November 5, 2010

Transportation Security Risk Management Risk Reduction



Metal Grating

Smoke Obscurant

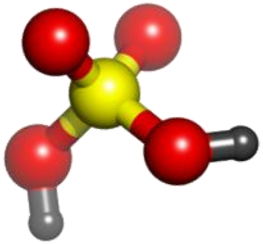


Container Tie Down

Photo credit: DOE NNSA Presentation, October 17-November 5, 2010

Transportation Security Risk Management
Risk Reduction

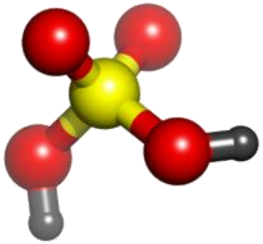
Photos: TSA User's Guide on Security Seals for Domestic Cargo



Transportation Risk Management

Selection of Transportation Contractor

- Evaluation of accident history and transportation safety plans
- Safety training of personnel
- Certifications/licensing
- Condition of equipment
- Confirm the following:
  - Secure packaging
  - Shipping documentation/bill of lading
  - Labelling
  - Safety data sheets
  - Appropriate PPE for spill response
  - Spill containment kits on board
  - Emergency Contact Information on board



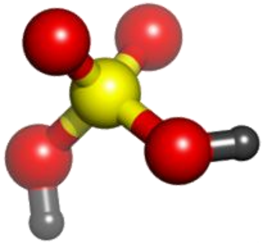
US Federal Motor Carrier Safety Regulations

The US FMCSA regulates:

- Driver qualifications
- Years of service
- Equipment standards
- Driving and parking rules
- Alcohol and controlled substances
- Financial responsibility
- Operational requirements

HAZMAT training required for:

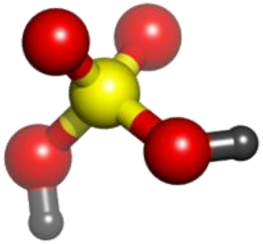
- Personnel who prepare, load/unload, or transport hazardous materials.



Balancing Transportation Security with Safety

Issue	Safety	Security
Placards	Commodity information needed by emergency responders to react appropriately to an accident and minimize any impact.	Commodity information could be used by terrorists to target specific chemicals.
Rerouting	May result in more accidents if there are longer transits or the infrastructure along an alternate route may be less well maintained or contain undesirable features (uncontrolled intersections, no shoulders, etc.).	Eliminating a shipment near a specific location (most likely a highly populated or critical area) may inadvertently transfer the risk from one community to another.

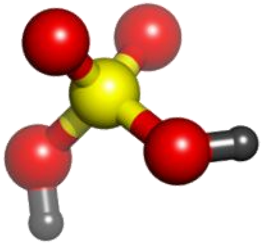
CCPS (2008). *Guidelines for Chemical Transportation Safety, Security, and Risk Management*



Balancing Transportation Security with Safety

Issue	Safety	Security
Working with supply chain partners (implementing security countermeasures)	Technology can be used for both safety and security (e.g., GPS to indicate location en route, emergency response to accident, and monitoring time-sensitive chemicals/materials).	Technologies focused on security should not distract the main function of the carriers (e.g., the safe transport of chemicals from point A to B).
Risk Analysis Methods	• Rational and structured results lead to recommendations • Participation and engagement by individuals with different perspectives, roles, and backgrounds/skill sets for safety, security, and transportation • Similar methodology • Same decision metrics (guidelines)	

CCPS (2008). *Guidelines for Chemical Transportation Safety, Security, and Risk Management*

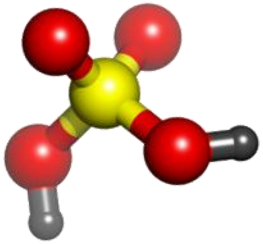


Transportation Risk Management
Evaluate

Example -

- A company ships a hazardous chemical from Factory A to Factory B.
- There are two different roads that connect Factory A and B.
- One road (Route 1) is in very poor condition and goes through a heavily populated part of City, but the distance to Factory B is shorter.
- The other road (Route 2) is in better condition, does not go through any populated areas, but the distance to Factory B is longer and takes more time.

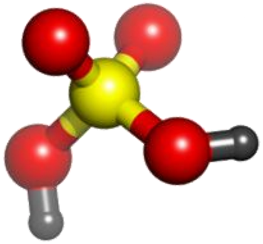
Photo: US National Transportation Safety Board



Transportation Risk Management
Evaluate

Example….

- A review of the transport logs shows that trucks traveling along Route 1 experience a breakdown or minor accident one time in about every 20 trips. However, no major chemical spill has resulted yet.
- The company has done a analysis and has concluded that 1 in every 50 accidents a truck will overturn and its hazardous cargo could spill.
- The company has decided that this is an unacceptable risk based on their evaluation criteria.



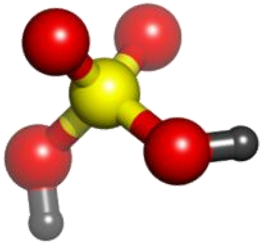
Transportation Risk Management
Reduction

Example….

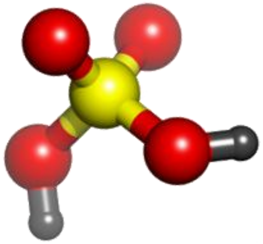
The company has decided that Route 1 is an unacceptable risk to the local population and will begin using Route 2 even though the distance is longer and takes more time.

Summary

- Chemical Transportation
- Case Study Involving the Shipment of Lithium Batteries
- Chemical Transportation Risk Management - Safety
  - Resources to help manage risks
  - Identify, analyze and reduce risks
- Chemical Transportation Risk Management - Security
  - Resources and Regulations
  - Identify, analyze and reduce security risks



TEA BREAK!



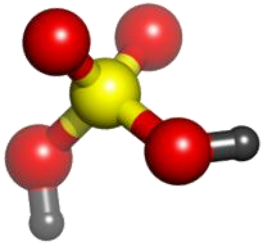
Principles of Security

SAND No. 2012-1606C
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

CSP
CHEMICAL SECURITY
ENGAGEMENT PROGRAM

SAND 2012-5234C

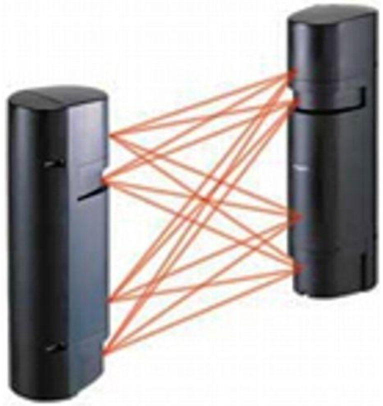
Sandia
National
Laboratories



Objectives

- Review the Definition and Objective of Security
- First Steps - Security Awareness
- Describe four Principles of Security
- Impart the importance of Performance-Based Security
- Provide a Model for a Systematic Approach to Security

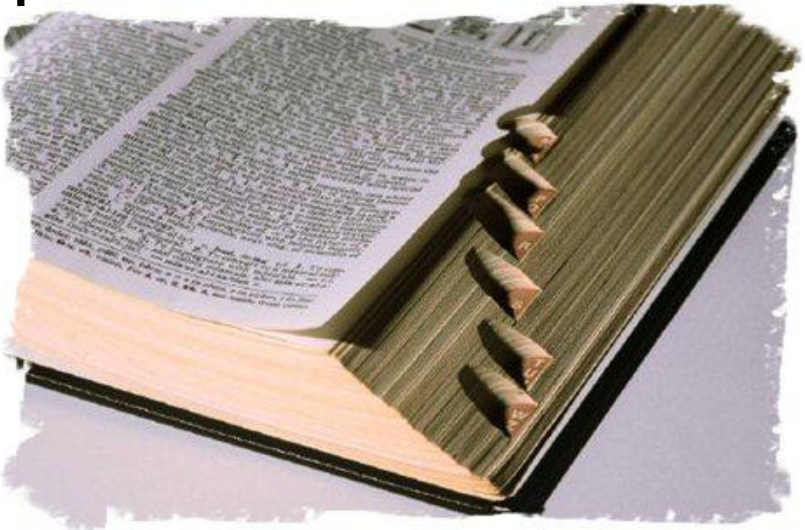
What is security?



Security Definition

Security is:

a combination of *technical* and *administrative* controls to deter, detect, delay, and respond to an *intentional*, *malevolent* event

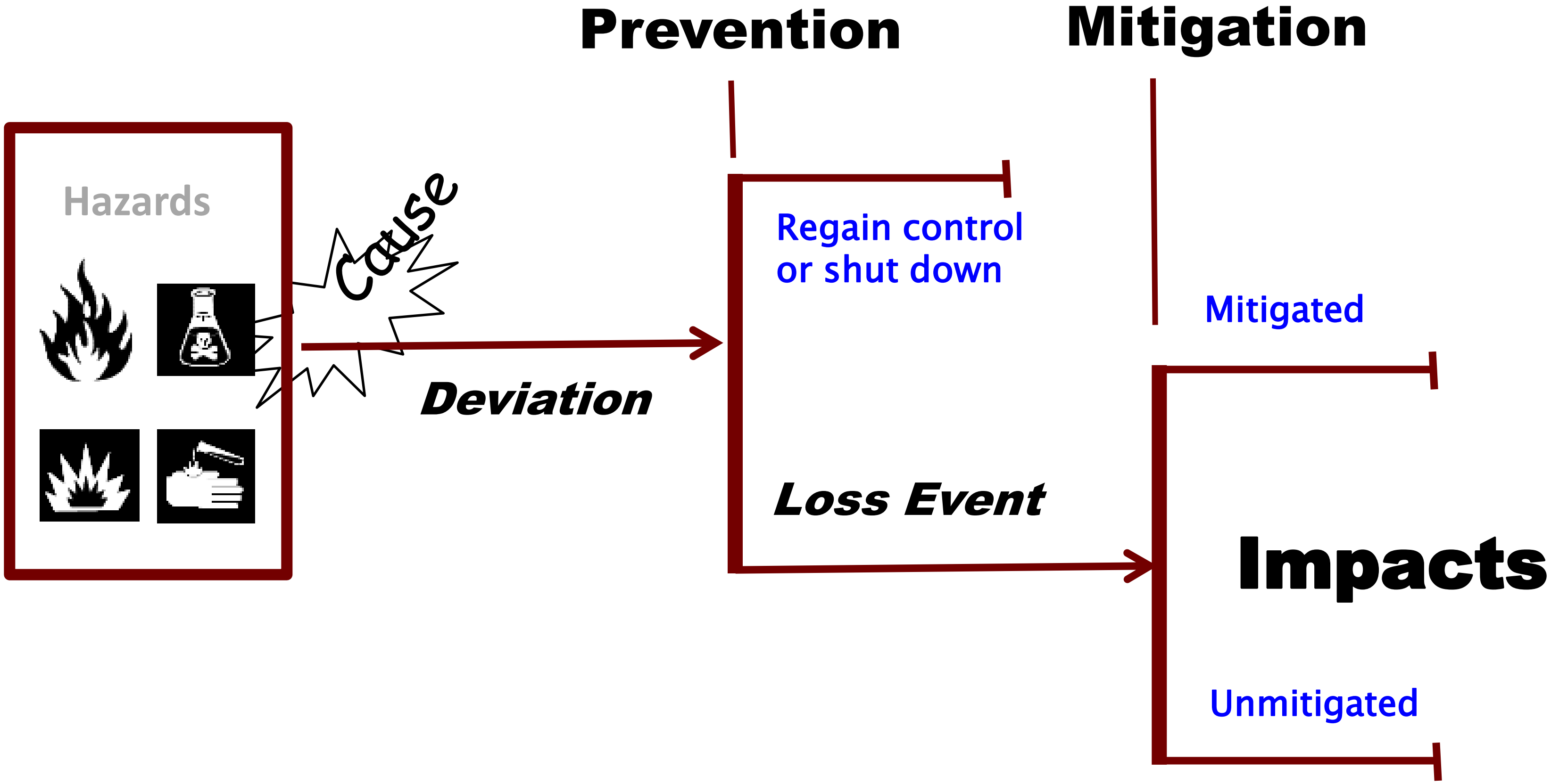


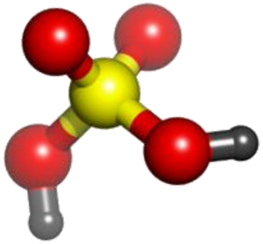
Security Objective

Security intends to prevent *intentional acts* which could result in unacceptable consequences

- Death/Severe Injury
- Chemical contamination
  - People
  - Environment
- Political Instability
- Economic Loss
- Industrial capacity loss
- Negative public psychological effect
- Adverse media coverage

Process Security is Similar to Process Safety





First Steps in Chemical Security: Low Cost Principles

Chemical Security Awareness

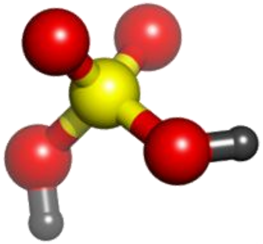
- Property-Vehicles-Information-Personnel
- Work Area - Changes
- Behavior - Suspicious
- Procedures - Followed

Access Controls

Have (credential), Know (PIN), Are (biometric*)

Manual (guards), Automated (machines)

* Can be expensive

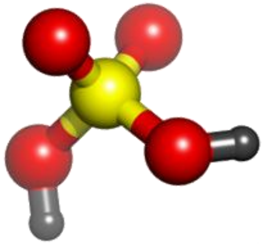


Basic Security Awareness

- Work area changes
  - Hole in fence
  - Suspicious packages
  - Inventory discrepancy
  - Door unlocked
- Symptoms of others behavior who are attempting to compromise security
  - Elicitation
  - Surveillance
  - Ordering supplies

Security awareness is the first step to making your facility safe from malevolent acts

Source: DHS Chemical Security Awareness Training



Awareness– Suspicious Behaviors

- Testing security – walking into, wait for discovery
- Mapping, loitering, staging vehicles
- Taking pictures of security system
- Looking in dumpster
- Trying to enter on your credential
- Asking for user name over the phone or by email
- Asking about plant layout – workers names – schedules

Source: DHS Chemical Security Awareness Training

Security Involves Systematic Diligence– even in Small Things

- Missing badge
- Leaving workstation unsecured - fire alarm
- Leaving sensitive document
- Bypassing security

Know what to do - who to call

Communicate anything unusual to supervisor

Remember - YOU are the first responder

Source: DHS Chemical Security Awareness Training

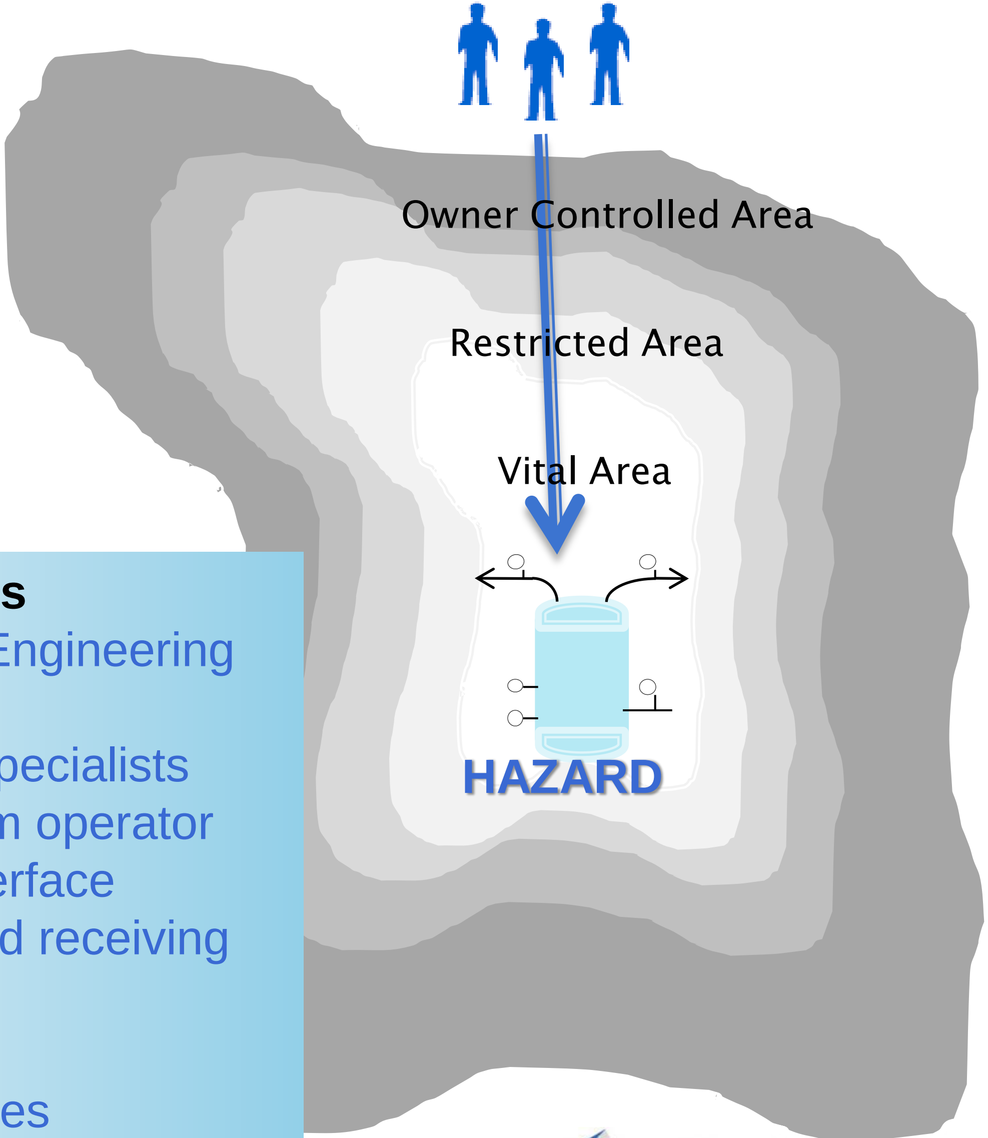
Access Control Integrated with Areas and People

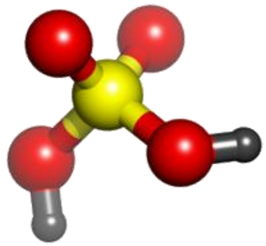
Plant locations

- Administration
- Control rooms
- Server rooms
- Switchgear
- Process Units
- Rail / truck yards
- Stores

Plant employees

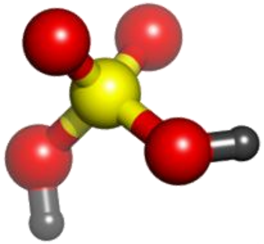
- Administration /Engineering
- Operations
  - Computer specialists
  - Control room operator
  - Process interface
  - Shipping and receiving
- Maintenance
- Security / Safety
- Special employees



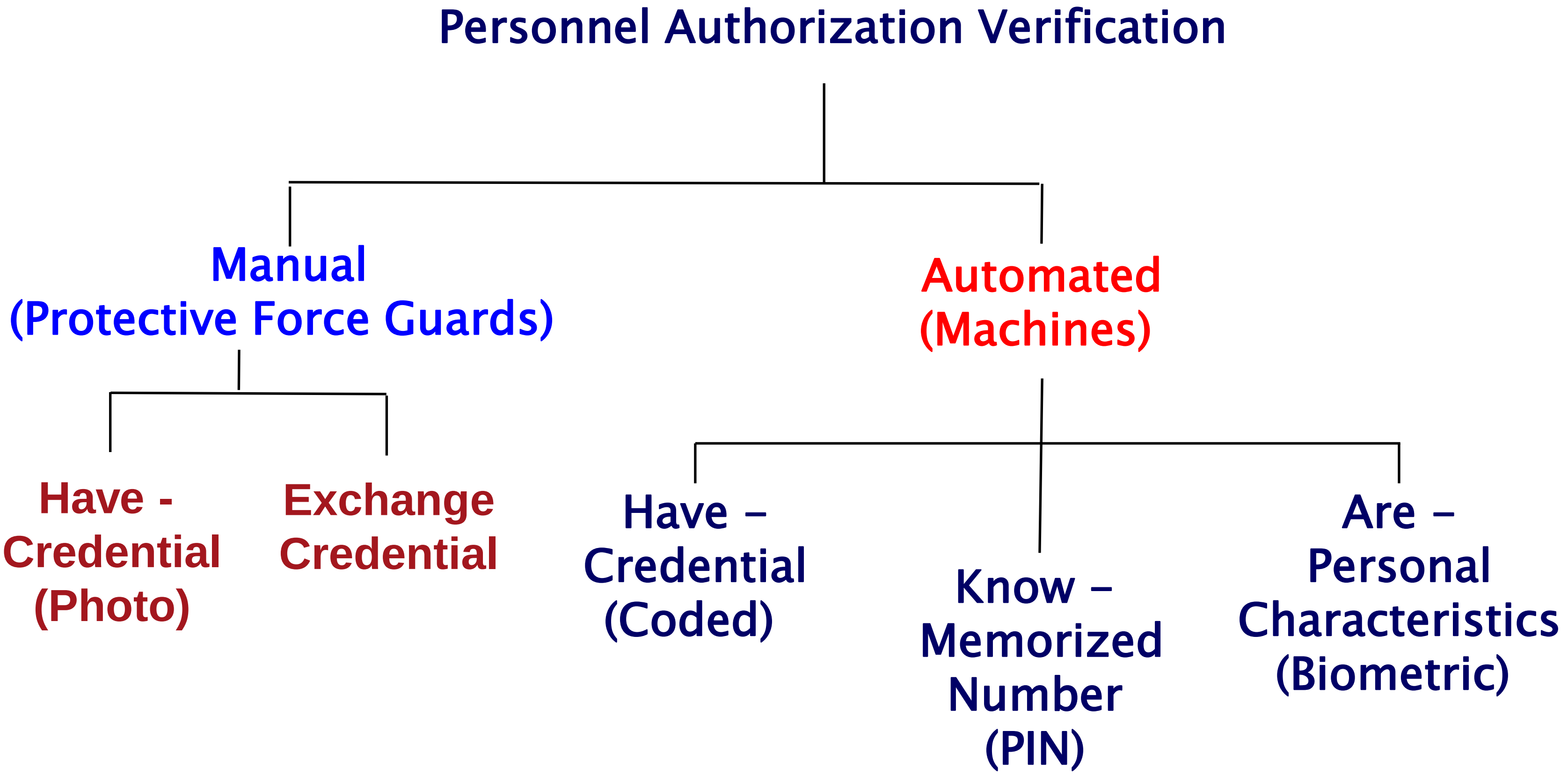


Features of a Good Entry Control System

- Integration with boundary
  - Cannot be bypassed
  - Block individuals until access authorization verified
  - Interfaces with the alarm system
- Integration with the guards/response force
  - Protects guard
  - Area is under surveillance
- Personnel integrate with system
  - Easy to use for entry and exit
  - Accommodates peak throughput (loads)
  - Accommodates special cases



Types of Personnel Entry Control



Personnel Authorization Verification

Manual
(Protective Force Guards)

Have - Credential (Photo)

Exchange Credential

Automated
(Machines)

Have – Credential (Coded)

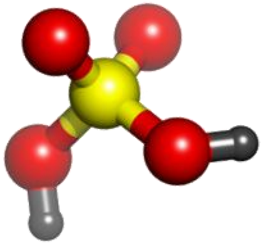
Know – Memorized Number (PIN)

Are – Personal Characteristics (Biometric)

What Kinds of Chemical Facilities Need Security?

Potential consequence severity will determine which facilities need to be secured

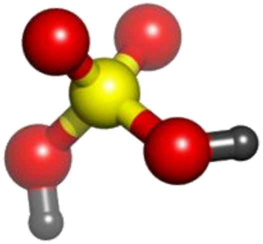
- Small-scale research laboratories
  - Many different chemicals used in small amounts
- Large-scale manufacturing plants
  - Limited types of chemicals used in large amounts



Chemical Industry Security Based on Theft, Release, and Sabotage

- Risk to public health & safety release
  - In-situ release of toxic chemicals
  - In-situ release and ignition of flammable chemicals
  - In-situ release/detonation of explosives chemicals
- Potential targets for theft or diversion
  - Chemical weapons and precursors
  - Weapons of mass effect (toxic inhalation hazards)
  - IED precursors
- Reactive and stored in transportation containers
  - Chemicals that react with water to generate toxic gases

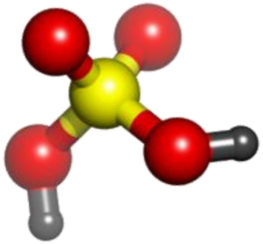
Source: DHS Chemical Security



Principles of Physical Security

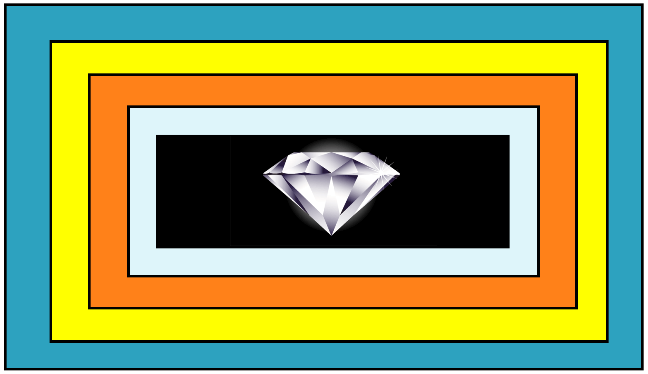
General Principles followed to help ensure effective, appropriate security

1. Defense in Depth
2. Balanced Security
3. Integrated Security
4. Managed Risk

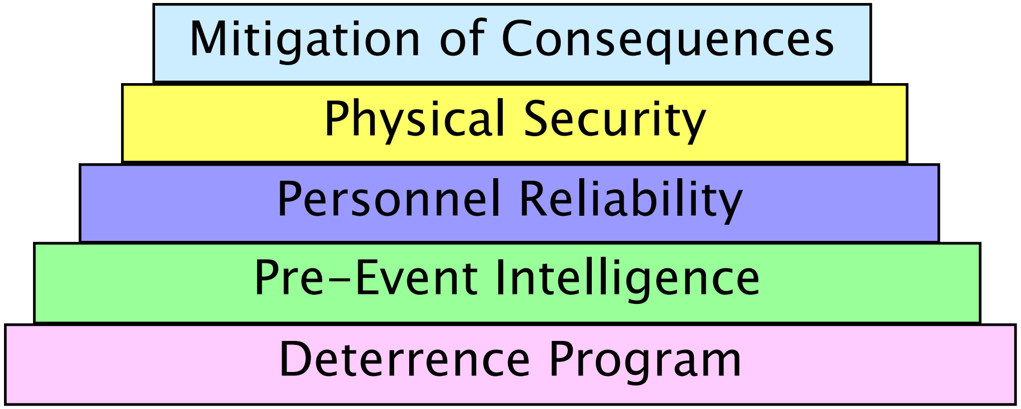


Principle 1: Defense in Depth

- Layers
  - Physical



  - Administrative and Programmatic



Mitigation of Consequences

Physical Security

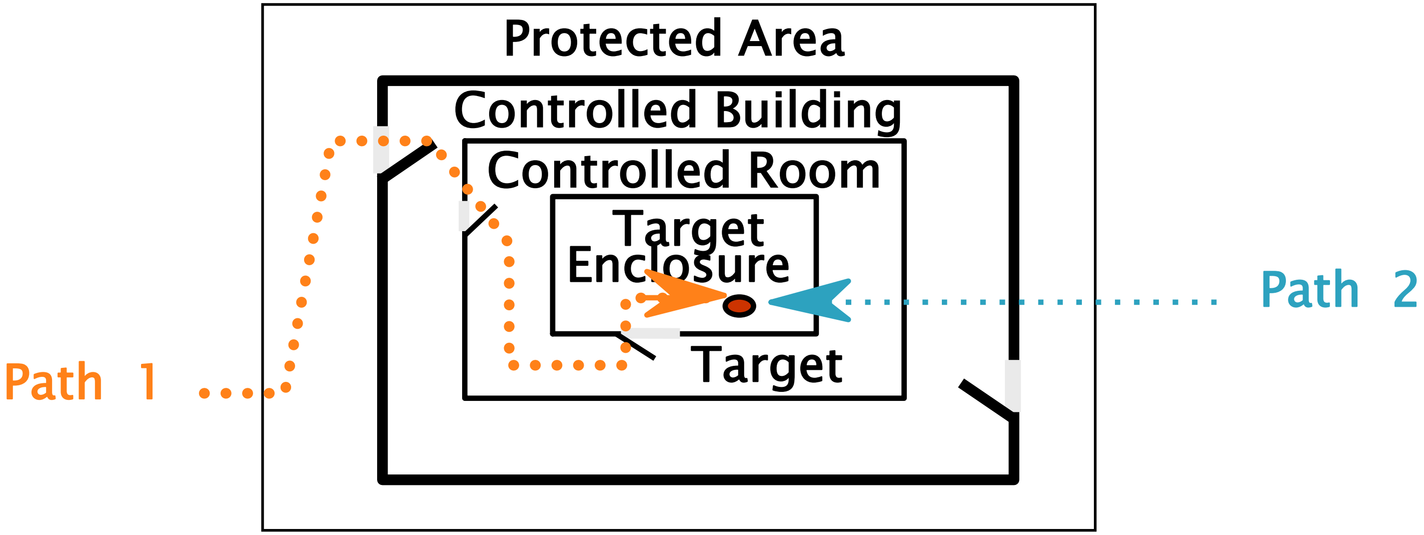
Personnel Reliability

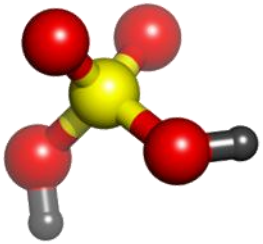
Pre-Event Intelligence

Deterrence Program

Principle 2: Balanced Protection

- Physical Layers
- Adversary Scenarios
  - Adversary paths (physical)





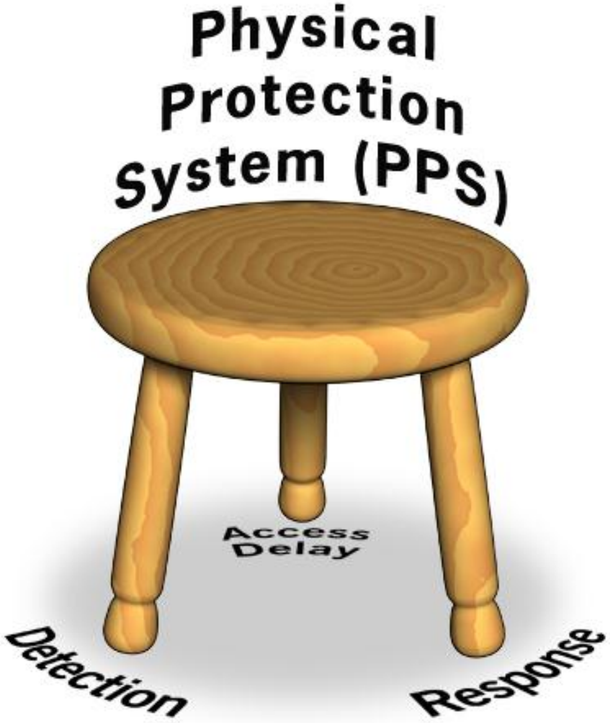
Balanced Protection

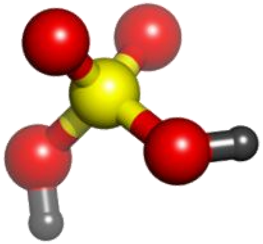
- Each Path is composed on many protection elements
  - Walls, fences, sensors, cameras, access controls, etc…
- Protection elements each possess delay and detection components
  - For example:
    - Fence delays adversaries *20* seconds, and provides 50% likelihood that adversary is detected
    - Wall delays adversary 120 seconds and provides a 10% likelihood of detection
    - Guard delays adversary 20 seconds and provides a 30% likelihood of detection
- Balanced protection objective:
  - for every possible adversary path
  - cumulative detection and delay encountered along path will be the similar
  - regardless of adversary path

  - NO WEAK PATH

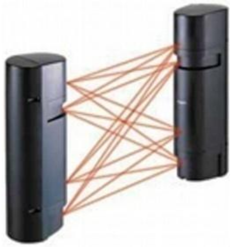
Principle 3: System Integration

- Detection alerts Response
- Access Delay slows the adversary to provide time for Response
- Response prevents the consequence





Integrated Security



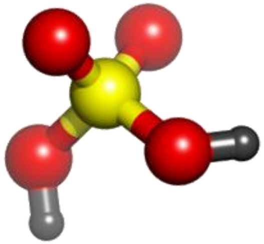
- Contribution to security system of each can be reduced to its contribution to:
  - Detection of adversary or malevolent event
  - Delay of adversary
  - Response to adversary
- Integrated security evaluates composite contribution of all components to these three elements
  - Assures that overall detection is sufficient and precedes delay
  - Assures that adversary delay time exceeds expected response time
  - Assures that response capability is greater than expected adversary

Principle 4: Managed Risk

- How much Security is enough ???

Cost of Security

Benefit of Security

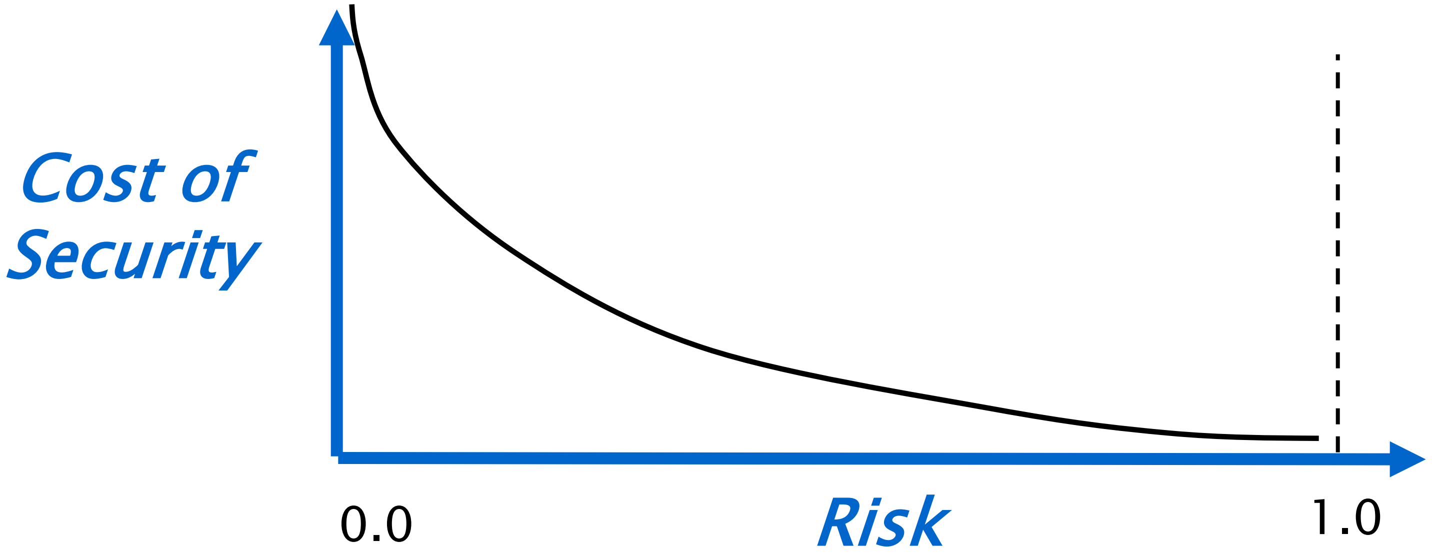


Managed Risk

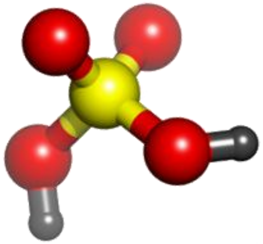
- Benefits of Security is Reduced Risk
- What is Risk?
  - Risk = Consequence Severity * Probability of Consequence
- What is Security Risk?
  - Probability of Consequence Occurrence ⇒
    - Frequency of attempted event

      X
    - Probability of successful attempt
  - Probability of successful attempt is
    - 1 - Probability of security system effectiveness

Managed Risk



- The benefit (risk reduction) increases with increased security investment (cost)
- However, there is a point where the increased benefit does not justify the increased cost



Managed Risk

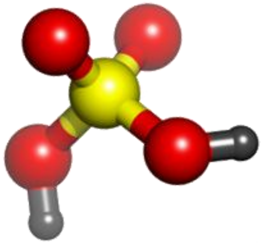
- How much Security is enough ???

Government Decision based on Managed Risk

Cost of Security

Level of Risk acceptable

Provides sufficient confidence that materials appropriately protected

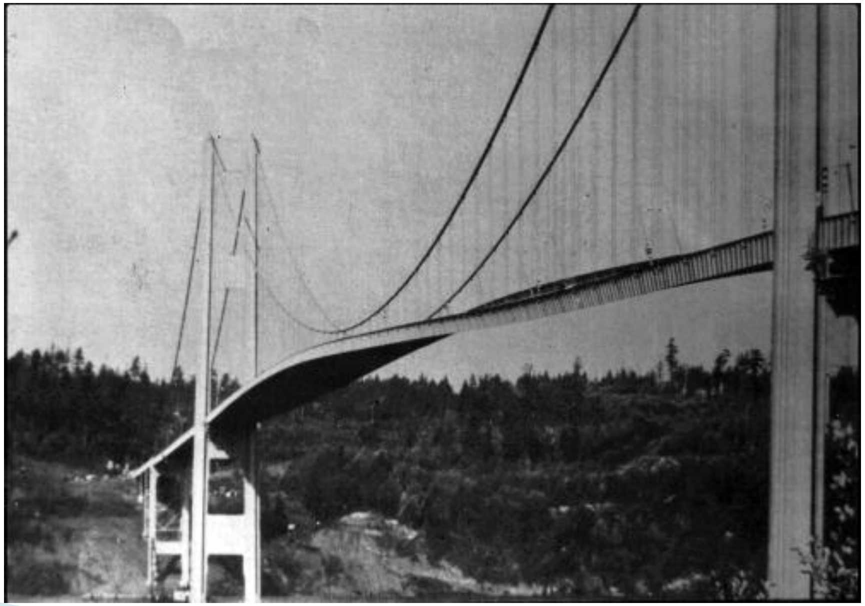


Objectives

- Review the Definition and Objective of Security
- First Steps – Security Awareness
- Describe Four Principles of Security
- Impart the Importance of Performance-Based Security
- Provide a Model for a Systematic Approach to Security

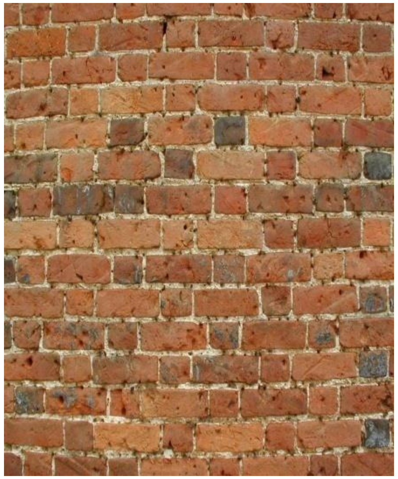
Performance-Based Security

- Requirements Driven
- Engineering Principles used for Security
  - What are requirements for system?
  - What are constraints of system?



Requirements-Driven Security

- Design Constraints
  - Understand Operational Conditions
- Design Requirements
  - Consequences to be prevented
    - Identify Targets to be protected
  - Define Threats against which targets will be protected



Operational Conditions

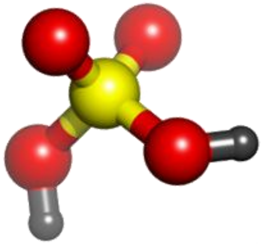
Characterize the facility considering:

- Mission
- Operations
- Budget
- Safety
- Legal Issues
- Regulatory Issues

Target Identification

What are the unacceptable consequences to be prevented?

- Death/Severe Injury
- Chemical contamination
  - People
  - Environment
- Political Instability
- Economic Loss
- Industrial capacity loss
- Negative public psychological effect
- Adverse media coverage



Target Identification

What are possible sources of unacceptable consequences?

- Dispersal
  - Identify areas to protect
- Theft
  - Identify material to protect

Target Identification

Characterize Types of Targets

- Form
- Storage manner and location
- Flow of chemicals
- Vulnerability of Chemicals
  - Flammable
  - Explosive
  - Caustic

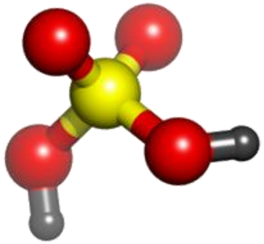
- **Criticality / Effect**
- **Access / Vulnerability**
- **Recoverability / Redundancy**
- **Vulnerability**

Define the Threats

The Art of War, Sun Tse

- If you know neither yourself nor your enemies, you will lose most of the time
- If you know yourself, but not your enemies, you will win 50%
- If you know yourself and your enemies, you will win most of the time

Knowing your threats permits proper preparation



The Physical Protection System Must Have a Basis for Design

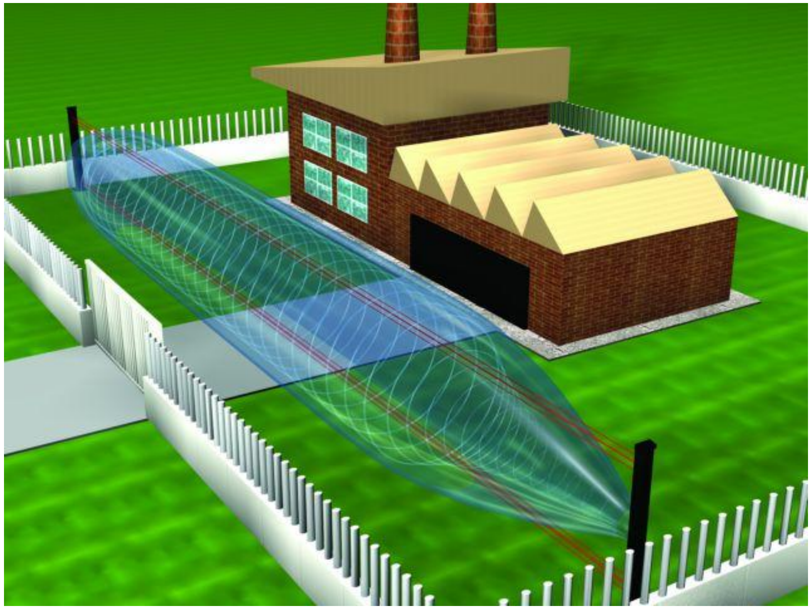
Threat Assessment: An evaluation of the threats- based on available intelligence, law enforcement, and open source information that describes the motivations, intentions, and capabilities of these threats

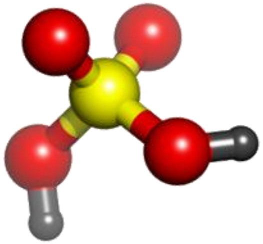
Design Basis Threat: A policy document used to establish performance criteria for a physical protection system (PPS). It is based on the results of threat assessments as well as other policy considerations

Define the Threats

In physical security:

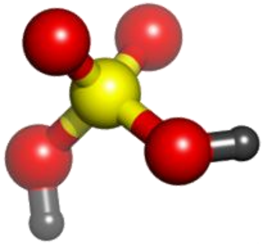
- Knowing adversary permits customizing security to maximize effectiveness
- As adversary not known, develop hypothetical adversary to customize security
- Hypothetical adversary description should be influenced by actual threat data





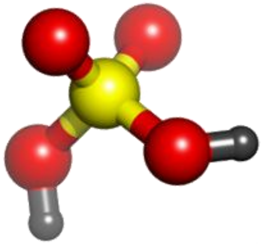
Design Basis Threat

- A Design Basis Threat (DBT) is a formalized approach to develop a threat-based design criteria
- DBT consists of the attributes and characteristics of potential adversaries. These attributes and characteristics are used as criteria to develop a customized security system design.
- The DBT is typically defined at a national level for a State.
- At the facility level, also:
  - Consider local threats
    - Local criminals, terrorists, protestors
  - Consider insider threats
    - Employees and others with access

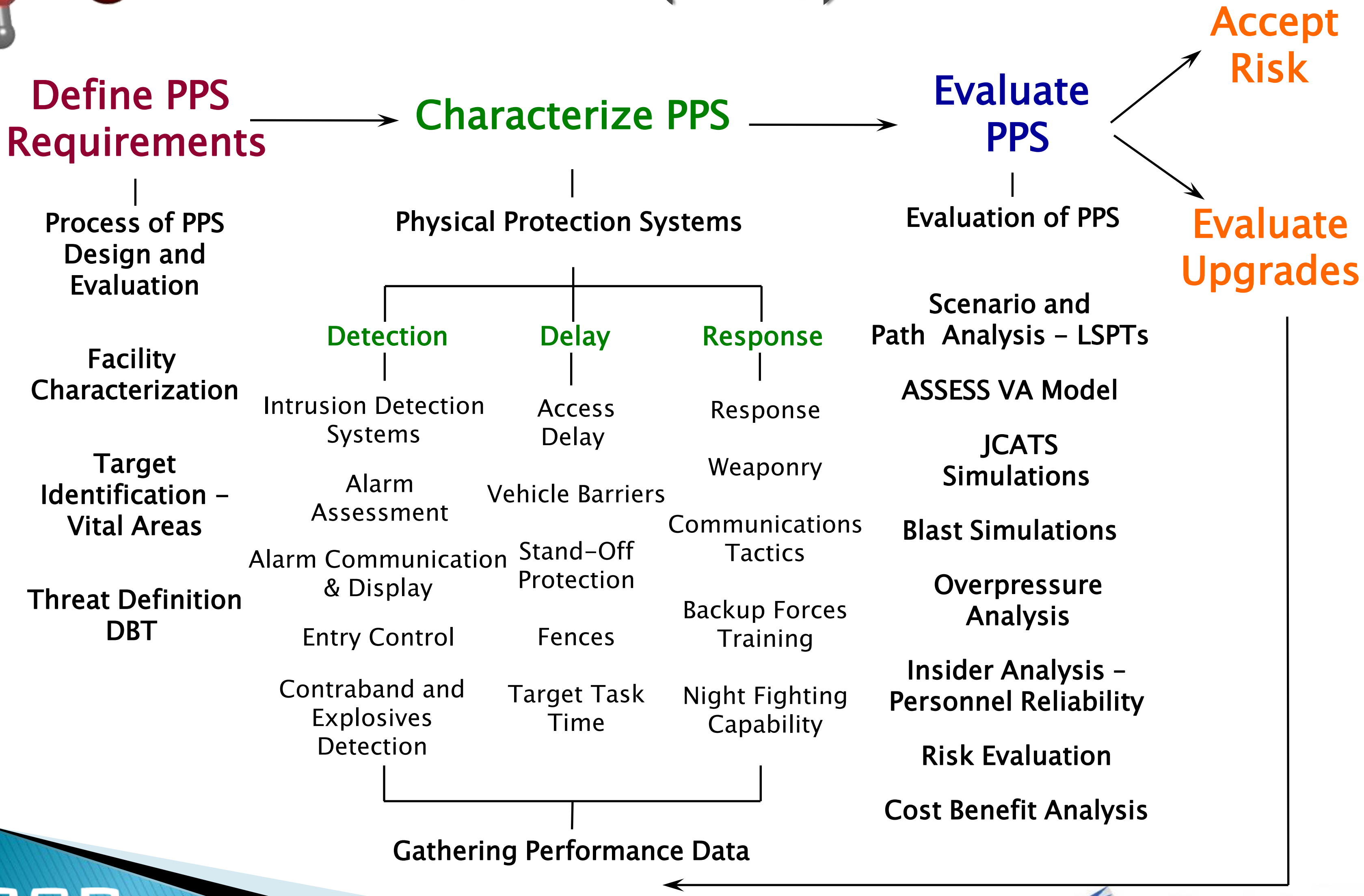


Objectives

- Review the Definition and Objective of Security
- First Steps – Security Awareness
- Describe the Principles of Security
- Impart the Importance of Performance-Based Security
- Provide a Model for a Systematic Approach to Security



Model: Design and Evaluation Process Outline (DEPO)



Define PPS Requirements

Process of PPS Design and Evaluation

Facility Characterization

Target Identification – Vital Areas

Threat Definition DBT

Characterize PPS

Physical Protection Systems

Detection

Intrusion Detection Systems

Alarm Assessment

Alarm Communication & Display

Entry Control

Contraband and Explosives Detection

Delay

Access Delay

Vehicle Barriers

Stand-Off Protection

Fences

Target Task Time

Response

Response

Weaponry

Communications Tactics

Backup Forces Training

Night Fighting Capability

Gathering Performance Data

Evaluate PPS

Evaluation of PPS

Scenario and Path Analysis – LSPTs

ASSESS VA Model

JCATS Simulations

Blast Simulations

Overpressure Analysis

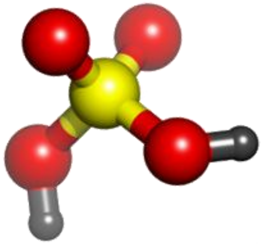
Insider Analysis – Personnel Reliability

Risk Evaluation

Cost Benefit Analysis

Accept Risk

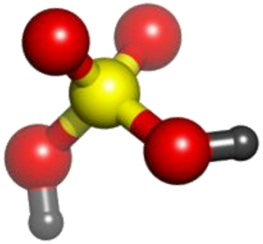
Evaluate Upgrades



Detect Adversary

- Technology
  - Intrusion Detection
  - Entry Control
  - Contraband Detection
  - Unauthorized Action Detection

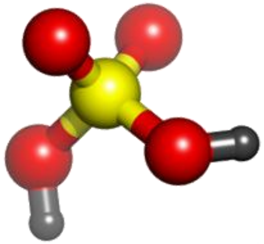
- Supporting elements
  - Alarm Assessment
  - Alarm Communication
  - Alarm Annunciation



Delay Adversary

Delay Definition :

- The element of a physical protection system designed to slow an adversary after they have been detected by use of
  - Walls, fences
  - Activated delays-foams, smoke, entanglement
  - Responders
- Delay is effective only after there is first sensing that initiates a response



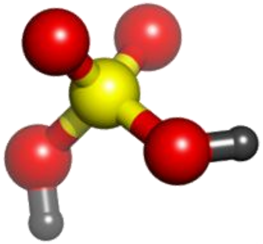
Respond to Adversary

Guard and Response Forces

Guards: A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or *transport*, controlling access. Can be armed or unarmed.

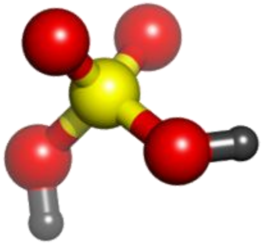
Response forces: Persons, on-site or off-site who are armed and appropriately equipped and trained to counter an attempted theft or an act of sabotage.

Guards can sometimes perform as initial responders as well (both guards and response force)



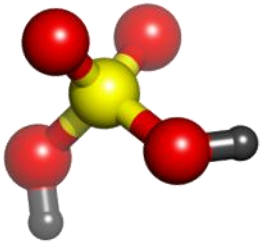
Summary

- Security systems should attempt to prevent, but be prepared to defeat an intentional malevolent act that could result in unacceptable consequences at a chemical facility
- Security awareness is an essential element
- An effective system depends on an appropriate integration of:
  - Detect
  - Delay
  - Respond



Summary

- Principles for security can lead to more effective security system
  - Defense in depth
  - Balanced security
  - Integrated security
  - Managed risk
- Performance-based approach will yield the greatest confidence that security is adequate
  - Threat criteria
- A model for systematic security design and analysis will enable application of principles and performance based approach



Cyber Security Standards and Best Practices

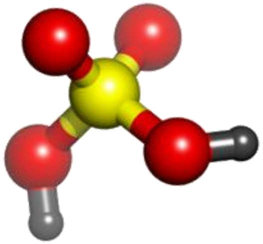
SAND No: 2012-**7255C**

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL850

CSP CHEMICAL SECURITY ENGAGEMENT PROGRAM

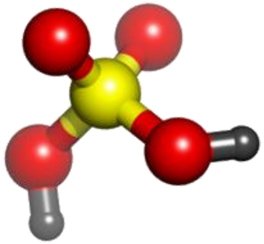
SAND 2012-5234C

Sandia National Laboratories



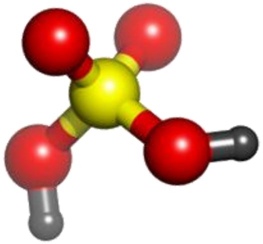
Presentation Overview

- Definitions and acronyms for cyber security
- Relevance of cyber security
- Cyber security protection methods
- Standards on cyber security
- Best practices in cyber protection methods
- Information recovery
- Case studies



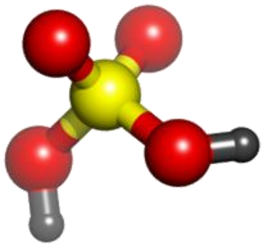
Common Acronyms

- APT – Advanced Persistent Threats
- DOS – Denial-of-Service
- IEC – International Electrotechnical Commission
- ISA – Industrial Society for Automation
- ISO – International Organization for Standardization
- NIST – National Institute of Standards and Technology
- NTK – Need-to-Know
- PDCA - Plan-Do-Check-Act
- PLC – Programmable Logic Controller
- SCADA – Supervisory Control and Data Acquisition systems
- SPDS – Safety Parameter Display System



Common Definitions

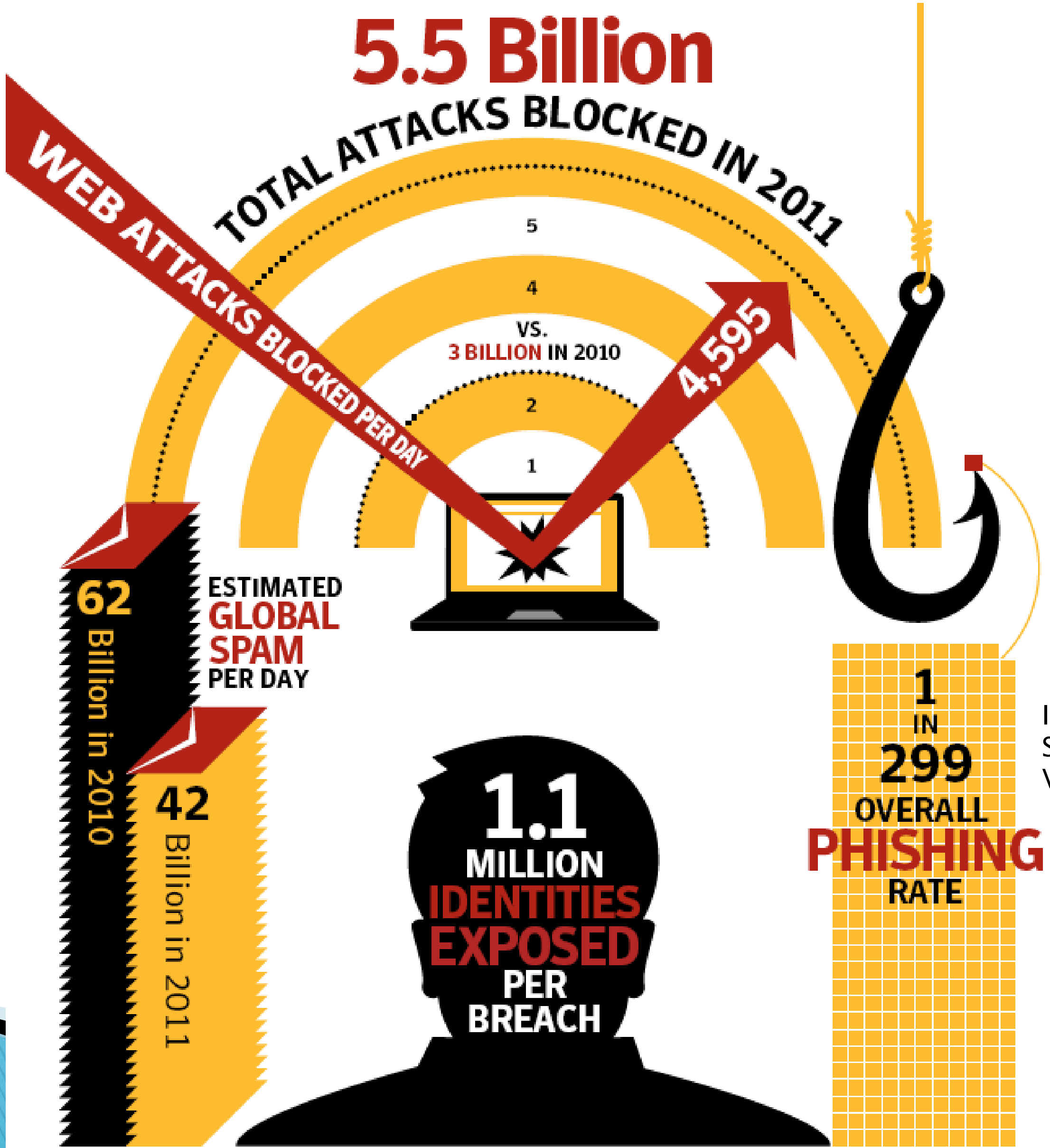
- **Anti-virus** – software used to prevent, detect, and remove malware
- **Firewall** – software or hardware used to keep a network secure by controlling incoming and outgoing system traffic
- **Hacking** – infiltrating computer systems and networks
- **Hacktivism** – use of computers and networks as a means of protest to promote political ends
- **Honeypot** – trap to detect, deflect, or counteract attempts at unauthorized use of information systems
- **Malware** – "malicious software" used to disrupt computer operation, gather sensitive data, or gain unauthorized access to a computer system



Common Definitions

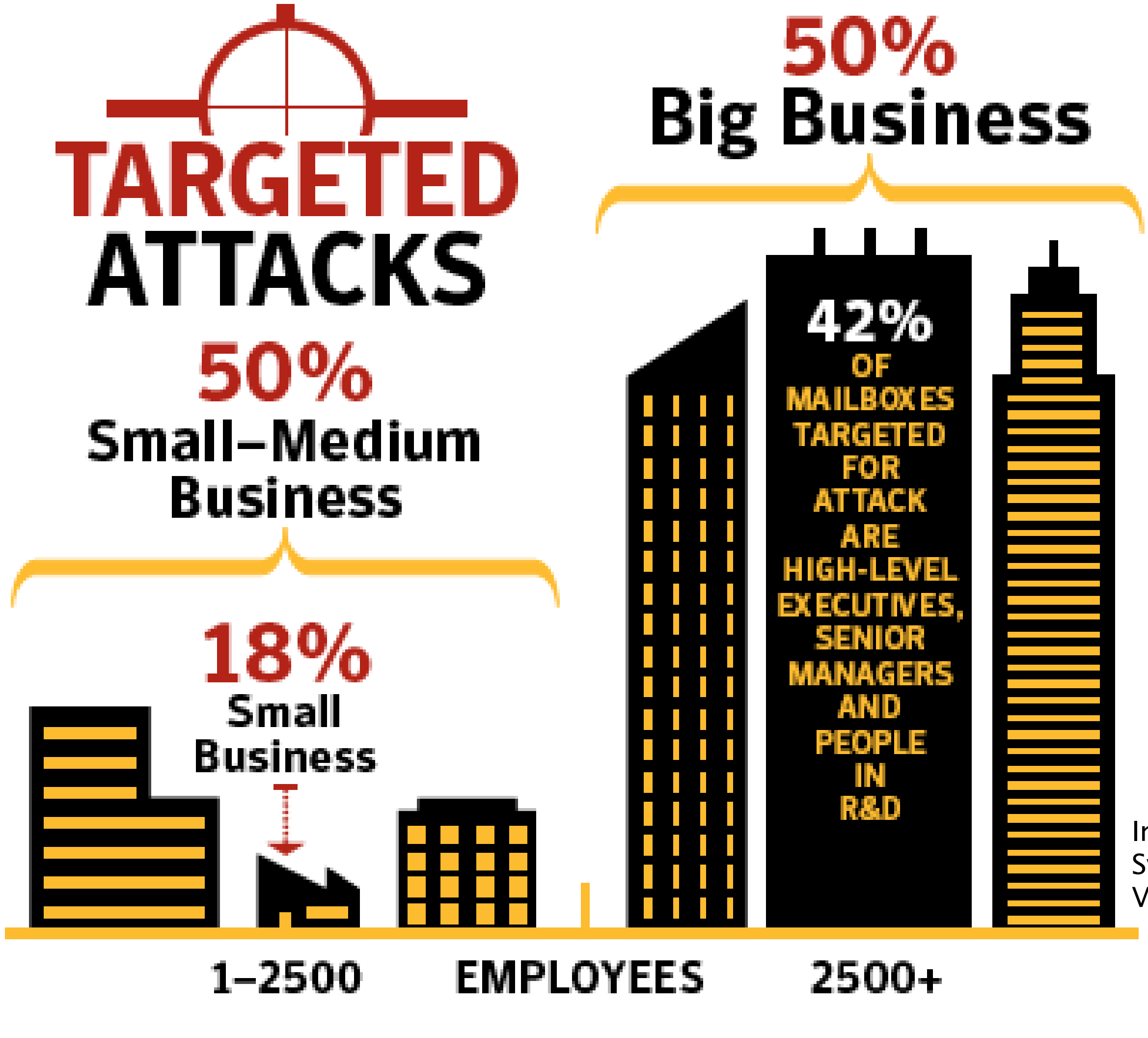
- **Phishing** – form of social engineering which attempts to acquire information (e.g., usernames, passwords, personal data) by mimicking trustworthy entities
- **Social engineering** – act of manipulating people into performing acts or divulging information
- **Spyware** – software that covertly gathers user information through an internet connection
- **Targeted attack** – customized malware and refined targeted social engineering to gain unauthorized access to sensitive information

Subject Relevance

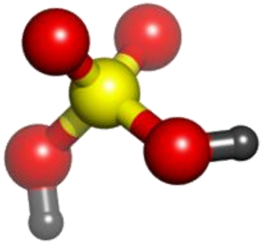


Internet Security Threat Report, Symantec, 2011 Trends, Volume 17, April 2012

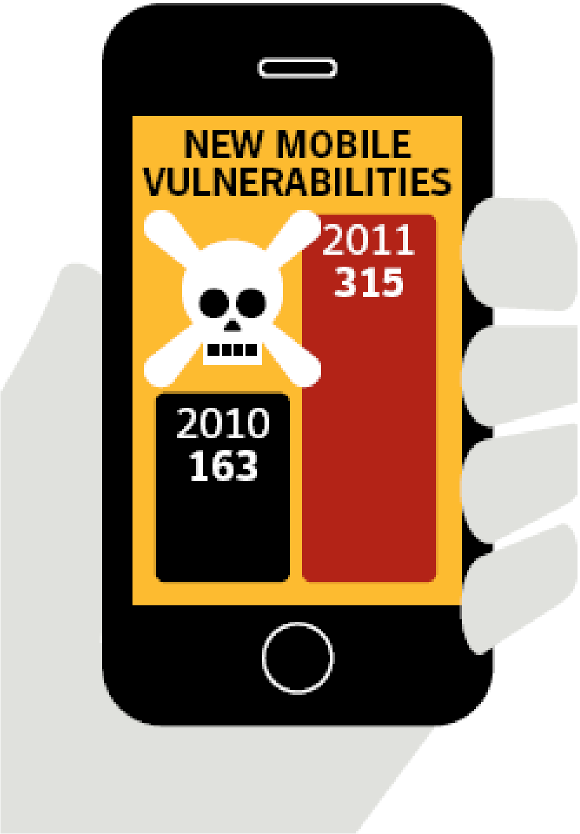
Subject Relevance

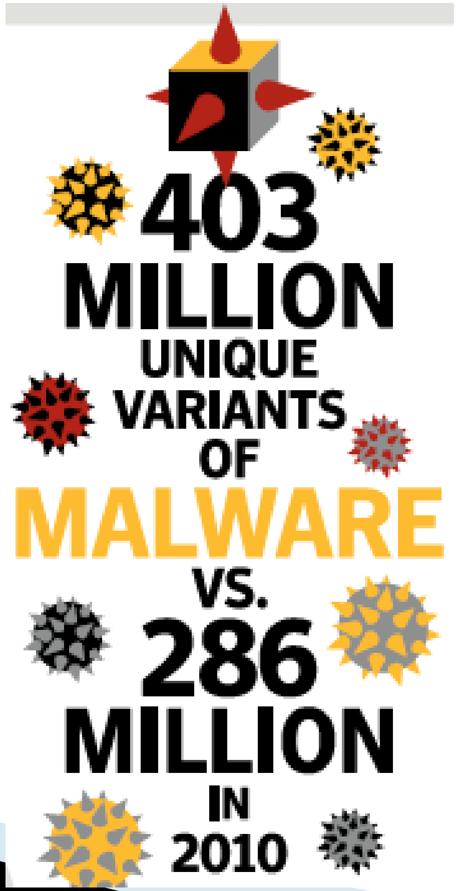


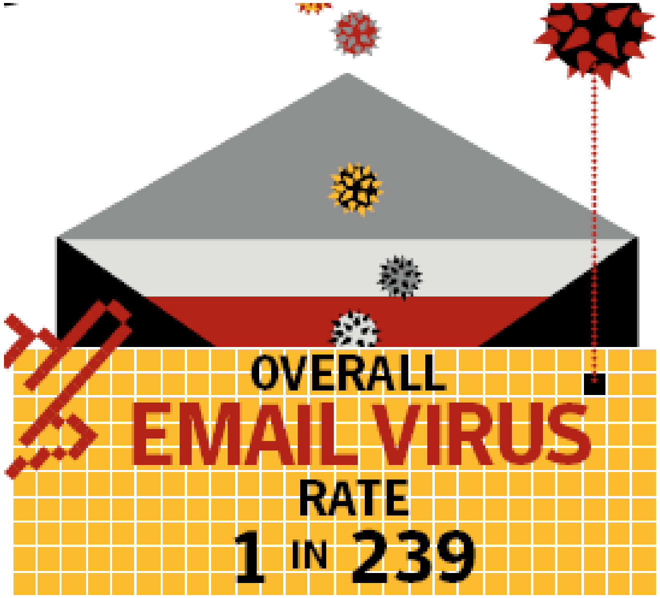
Internet Security Threat Report,
Symantec, 2011 Trends,
Volume 17, April 2012



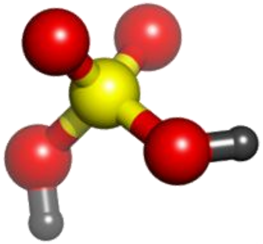
Subject Relevance





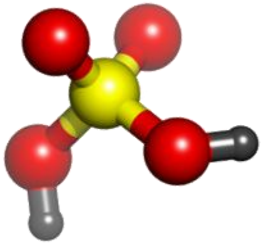


Internet Security Threat Report,
Symantec, 2011 Trends,
Volume 17, April 2012



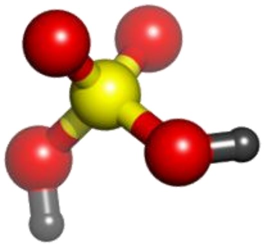
Subject Relevance

- Symantec Corporation blocked 5.5 billion malicious attacks in 2011, an increase of more than 81% from previous year
- Web attacks blocked per day increased by 36%
- Company executives, management, and research staff are no longer primary targets, 58% of attacks are going against other job functions
  - Example: Human resources or recruiters commonly receive resumes and curriculum vitae from applicants
- Mobile phones are being targeted
- 232 million identities stolen in 2011



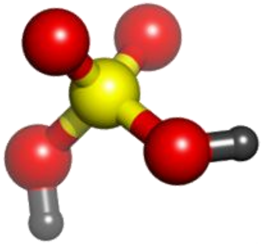
Cyber attacks

- Cyber attacks rely primarily on two methods
  - Malware
  - Hacking
- Use of these methods to exploit vulnerabilities, steal information, execute commands
- May be used in tandem
  - Malware may open a backdoor for hacker infiltration and theft
  - Hacker may exploit system weakness to install malware (e.g., keylogger)
- Social engineering techniques (e.g., phishing) are means to obtain private information (e.g., passwords) through human vulnerability and are gaining popularity



Types of Malware

- **Adware** – programs that secretly gather personal information and relay information to another computer, generally for advertising purposes
- **Rootkits** – tool used to gain administrator-level access to a computer
- **Spyware** – stand-alone programs that can secretly monitor system activity, passwords, and other data and relay information to another computer
- **Trojan horses** – seemingly desirable program that is malicious. User must invite the program into the computer (e.g., email attachment), the program does not replicate
- **Virus** – parasitic program written intentionally to enter a computer without user permission or knowledge which may then replicate and cause serious damage (e.g., file deletion) or effect system performance
- **Worms** – malware computer program that replicates itself in order to spread to other computers through security vulnerabilities



Types of Hackers

- **White hat** – security breakers for non-malicious reasons (e.g., test their personal security, working for a security software company)
- **Black hat** – violates computer security for little reason beyond maliciousness or personal gain
- **Grey hat** – combination of Black Hat and White Hat hackers, they hack into systems for the purpose of notifying administrators that their system was infiltrated with an offer to repair the system for a nominal fee
- **Blue hat** – someone who is used to bug test a system prior to launch, looking for vulnerabilities prior to launch
- **Elite hacker** – most skilled hackers who belong to a community that circulates new exploits
- **Script kiddie** – non-expert who breaks into a computer system using automated tools written by others

Types of Hackers

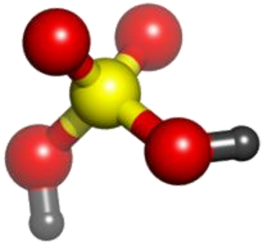
- **Hacktivist** – hacker who utilizes technology to announce a social, ideological, religious, or political message
- **Nation state** – intelligence agencies and cyberwarefare operatives of nation states
- **Organized criminal gangs** – gangs of hackers who attempt to gain financially
- **Bots** – automated software tools

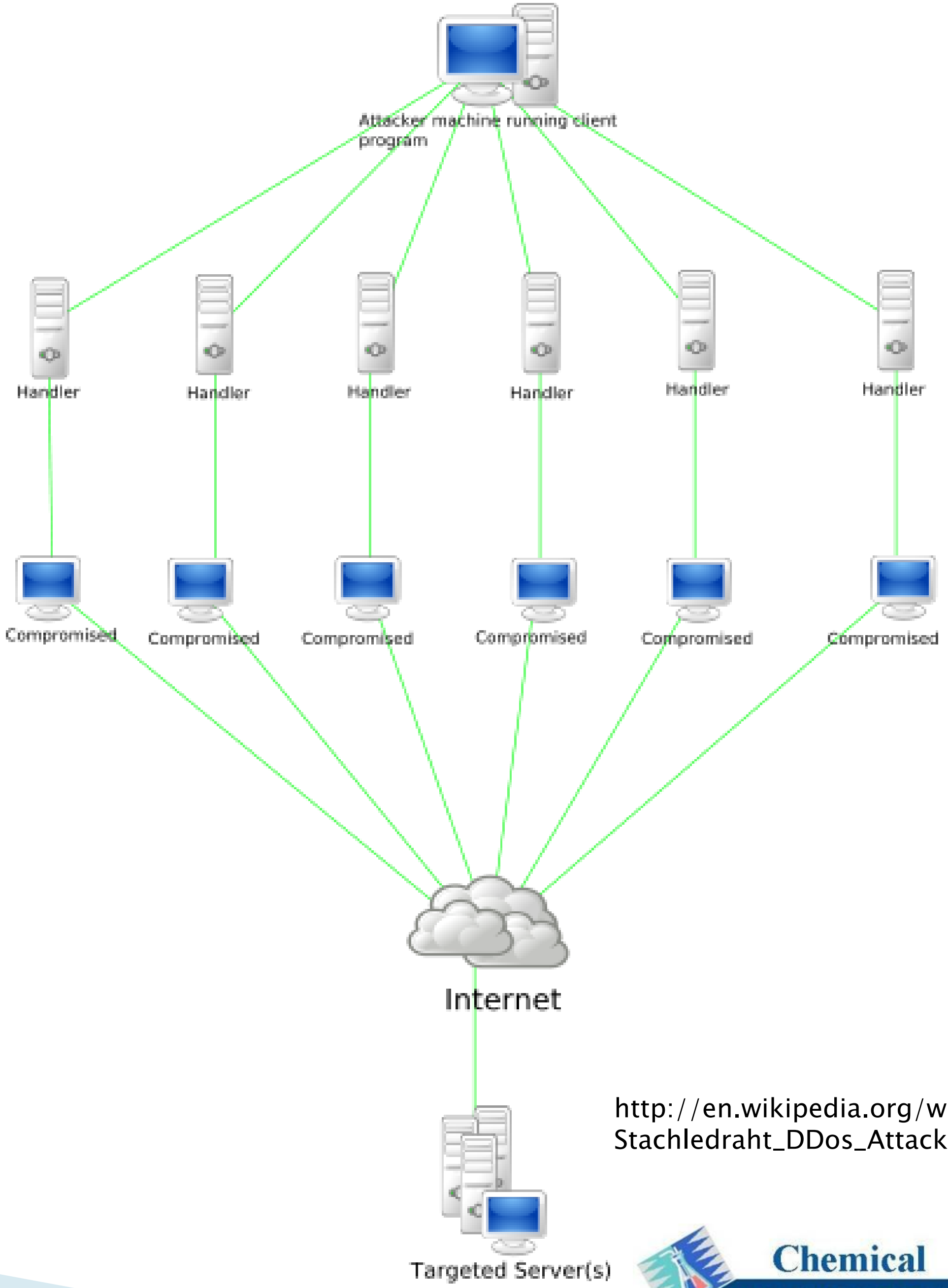
http://donthatethegeek.com/wp-content/uploads/2011/08/Hacker_d70focus_1.jpg

Types of Hacking Attacks

- **Network enumeration** – discovering information about the intended target
- **Vulnerability analysis** – identifying potential ways of attack
- **Exploitation** – attempting to compromise the system by employing the vulnerabilities found during a vulnerability analysis
- **Website defacement** – altering the visual appearance, product image, or content; common tactic amongst hacktivists
- **Denial-of-service attack (DOS)** – attempt to make a machine or network resource unavailable to intended users; saturate target with external communication such that it cannot respond to legitimate traffic

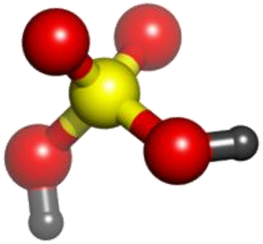
http://i1-news.softpedia-static.com/images/news2/Web-Defacement-Archive-Defaced-2.jpg





Denial-of-Service

http://en.wikipedia.org/wiki/File:
Stachledraht_DDos_Attack.svg

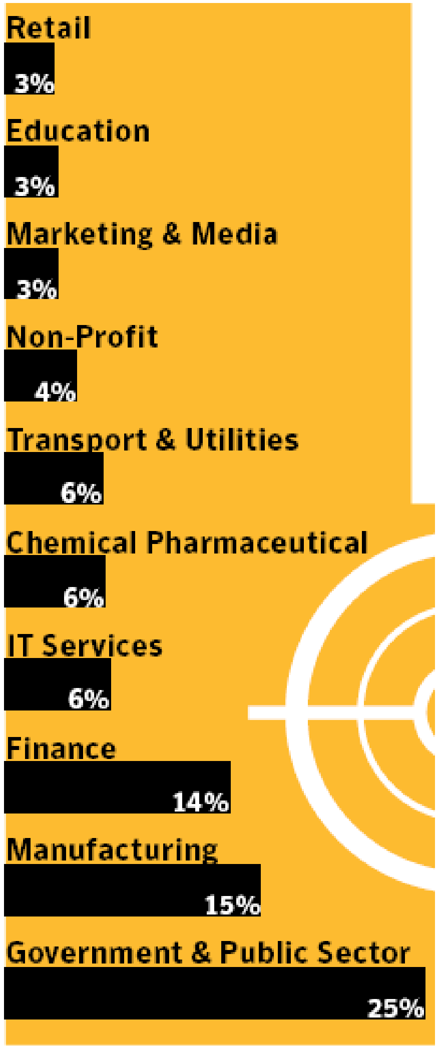


Cyber Espionage

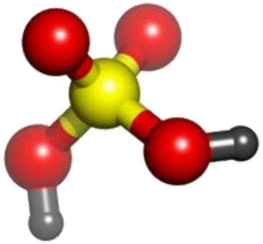
- According to Symantec Corporation, targeted attacks increased from 77 per day in 2010 to 82 per day in 2011
- Recent attacks include:
  - Stuxnet (2010)
  - Duqu (2011)
  - Flamer (2012)
- Hackivism groups, such as Anonymous and LulzSec, are growing in numbers and intent
- Attacks are growing significantly more sophisticated

Cyber Espionage

- In 2011, 29 companies in the chemical sector were targeted with emails that appeared to be from known suppliers
- These emails installed a well-known backdoor trojan with the intention of stealing valuable intellectual property
  - Design documents
  - Proprietary formulations



Internet Security Threat Report,
Symantec, 2011 Trends,
Volume 17, April 2012

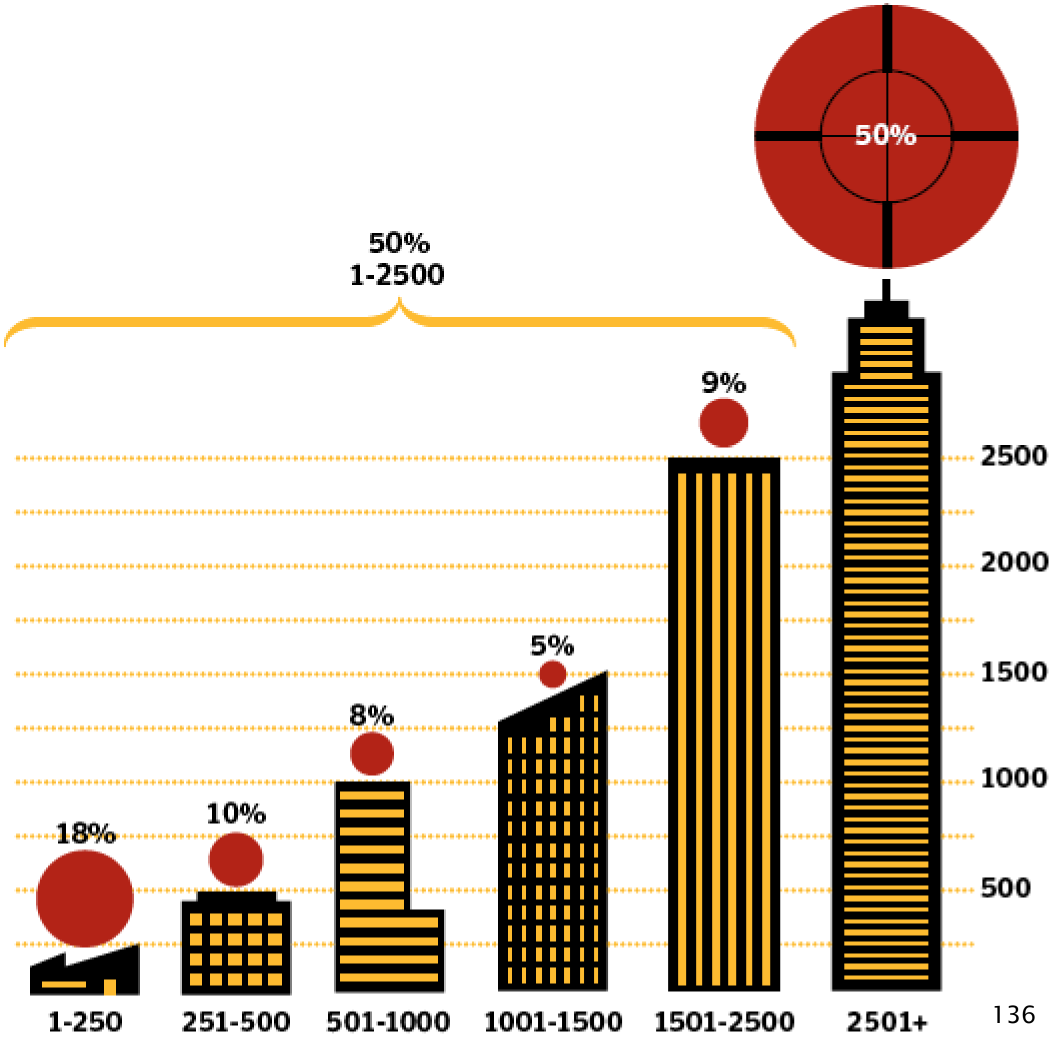


Cyber Espionage

- All sized companies are vulnerable
- Targeted recipients
  - Executive level (25%)
  - Senior level (8%)
  - Research (9%)
  - Shared mailbox (23%)
  - Sales (12%)
  - Media (10%)
  - Primary assistant (6%)
  - Recruitment (6%)

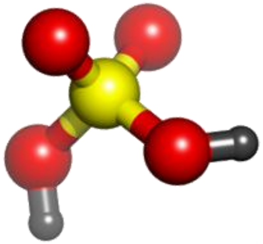
Figure 3

Attacks By Size Of Targeted Organization



Internet Security Threat Report,
Symantec, 2011 Trends,
Volume 17, April 2012

CSP
CHEMICAL SECURITY
ENGAGEMENT PROGRAM



Cyber Espionage

- Advanced Persistent Threats (APT)
  1. Highly customized tools and intrusion techniques
  2. Stealthy, patient, persistent methods to reduce the risk of detection
  3. Aim to gather high-value, national objectives such as military, political, or economic intelligence
  4. Well-funded, well-staffed, perhaps operating with the support of military or state intelligence organizations
  5. More likely to target organizations of strategic importance

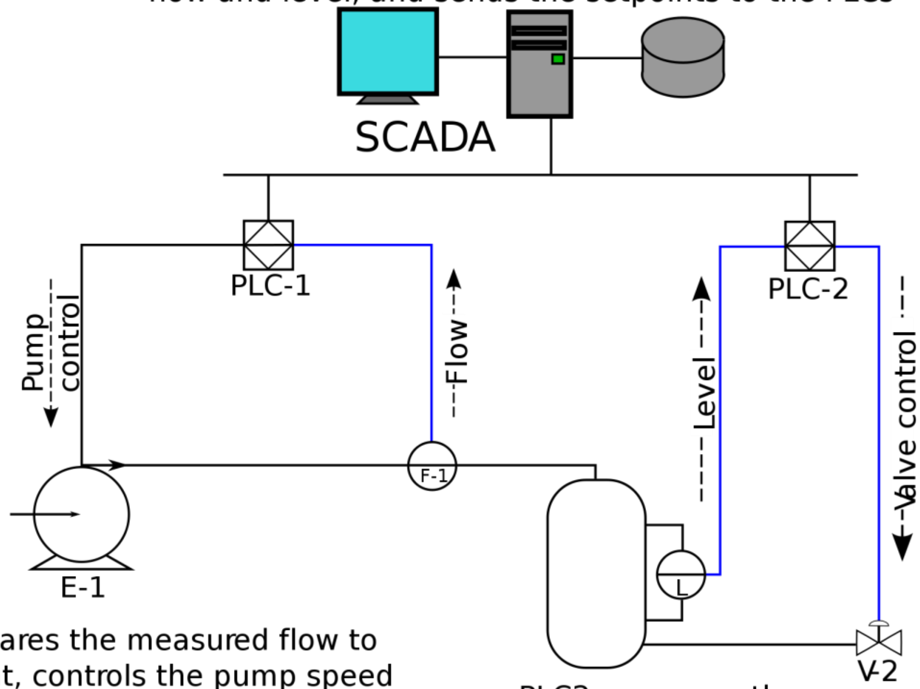
Cyber Espionage

- Targeting Supervisory Control and Data Acquisition (SCADA) systems
- SCADA systems rely heavily on Programmable Logic Controller (PLC)
- PLCs are a digital computer used for automation of electromechanical processes (e.g., communication, setpoints)
- In general, SCADA systems support
  - Processes that manage water supply and treatment plants
  - Electrical power distribution and transmission
  - Operate chemical and nuclear plants
  - Heating, Ventilation, Air Conditioning (HVAC)

Cyber Espionage

- Supervisory Control and Data Acquisition (SCADA) systems

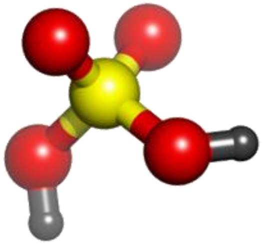
The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs



PLC1 compares the measured flow to the setpoint, controls the pump speed as required to match flow to setpoint

PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint

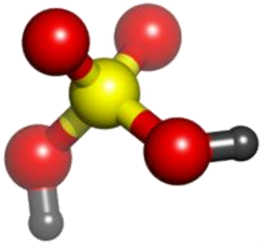
http://upload.wikimedia.org/wikipedia/commons/thumb/0/0c/SCADA_schematic_overview-s.svg/2000px-SCADA_schematic_overview-s.svg.png



Cyber Espionage

- What are some potential targets for Advanced Persistent Threats?

1.
2.
3.
4.
5.



Cyber Espionage

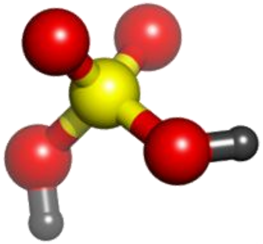
- What are some potential targets for Advanced Persistent Threats?

1. Defense contractors
2. Finance
3. Chemical industries
4. Manufacturing
5. IT services

Prevention of Cyber Attacks

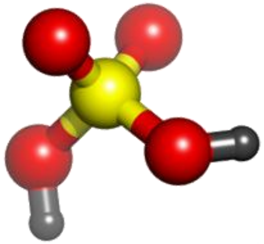
- Prevent cyber attacks
  - Cyber security standards
  - Best practices
  - Using resources to hire agencies to better protect critical systems, proprietary information, and private data

http://infiltrated.net/mgz/password-cracking.jpg



Cyber Security Standards

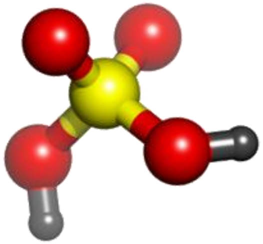
- ISO 27k Series
  - ISO 27001
  - ISO 27002
  - ISO 27032
- NIST (National Institute of Standards and Technology)
- ISA (International Society of Automation)
  - ISA-99 (Standards for Industrial Automation Control Systems)



ISO Standards

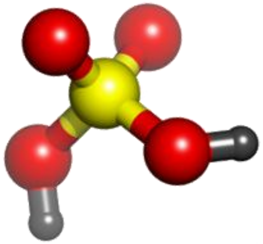
- ISO 27001: International Security Management Systems (ISMS) Requirements Standard

Formally specifies an information security management system (ISMS) for establishing, implementing, operating, monitoring, reviewing and maintaining an organizations information security risks



ISO/IEC 27001

- Defines and assigns information security roles and responsibilities throughout the organization
- Originated with British Standard 7799 in 1995. Incorporated as the ISO 27001 standard in 2005.
- Covers all types and sizes of organizations
- Currently under revision to align to other management system standards. Revised version likely available 2013

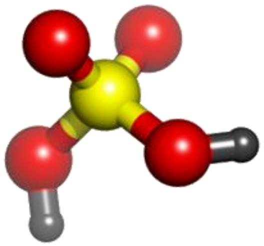


ISO 27001 Requirements

- Management shall:
  - Examine information security risks systematically, to include threats, vulnerabilities and consequences
  - Design and implement information security controls to address unacceptable risks identified
  - Adopt an overarching management process to ensure continuous improvement

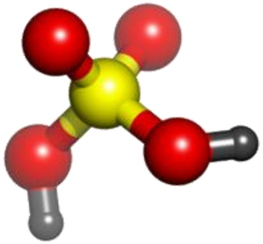
ISO International Organization for Standardization

http://www.iso.org/iso/home.htm



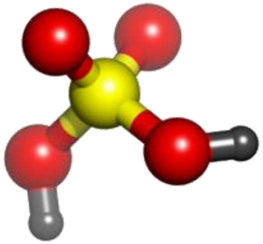
Features of ISO 27001

- Incorporates Deming's Plan-Do-Check-Act (PDCA) Process Model
- Thus, it aligns with ISO 9000 quality standards
- Is a process based approach
- Stresses continuous process improvement
- Annex A contains 39 control objectives and 133 information security controls
- Over 7000 organizations worldwide have been certified as compliant to ISO 27001
- There are equivalent national variants as well



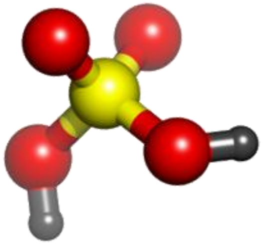
ISO 270001

As a management system standard, ISO 27001 requires that management controls be implemented. Specific information security controls are not specified, but rather applicable controls for each organization are selected based on each individual organization’s information security risks identified through the ISMS process



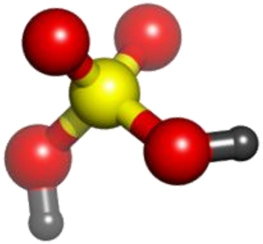
Benefits of ISO 27001

- Increased reliability and security of information systems
- Increased profits as a result of certification
- Cost-effective and consistent information security
- Systems rationalization
- Compliance with legislation
- Improved risk management and contingency planning
- Enhanced customer and trading partner confidence



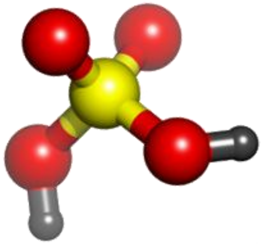
ISO/IEC 27002

- Currently entitled “Information Technology-Security Techniques-Code of Practice for Information Security Management
- Under revision; new version (due 2013) will likely be titled “Code of Practice for Information Security Codes”
- 27002 is not a certification standard like 27001 but an advisory code of practice



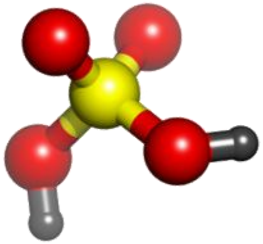
ISO/IEC 27002

- Concerned with information security, not just IT/systems security
- Describes a well defined set of suggested controls for ensuring:
  - Confidentiality
  - Integrity
  - Availability
- Specifies some 39 control objectives to comprise a generic functional requirements specification for information security management



ISO/IEC 27032

- Entitled “Preservation of Confidentiality, Integrity and Availability of Information in the Cyberspace”
- Cyberspace is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology, devices and networks connected to it, which does not exist in any physical form”



ISO/IEC 27032

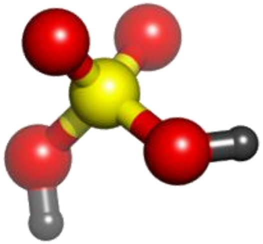
- Addresses:
  - Assets in the cyberspace
  - Threats against the cyberspace security
  - Cyber security controls
  - Various other issues

ISO/IEC 27032 is a Work-in-Progress. Version 1 expected to be released late 2012

ISO references

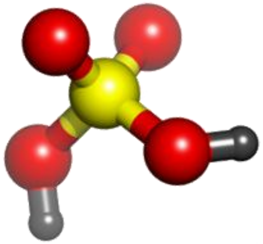
- http://www.iso.org/iso/home.html
- http://www.iso27001security.pl/html/iso27000.html
- http://www.iec.ch/

http://www.iso.org/iso/home.htm



NIST Standards

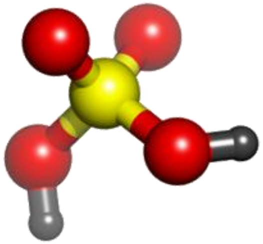
- NIST publication 800-12 “Computer Security Handbook”
- NIST Publication 800-14 “Generally Accepted Principles and Practices for Securing Information Technology”
- NIST Publication 800-26 “Security Self Assessment Guide to Information Technology Systems”
- NIST publication 800-53 addresses 194 security controls for IT systems



NIST References

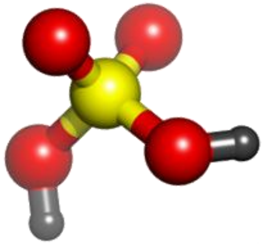
- http://www.nist.gov

http://nist.gov/itl/math/images/
NIST-Logo_5.jpg

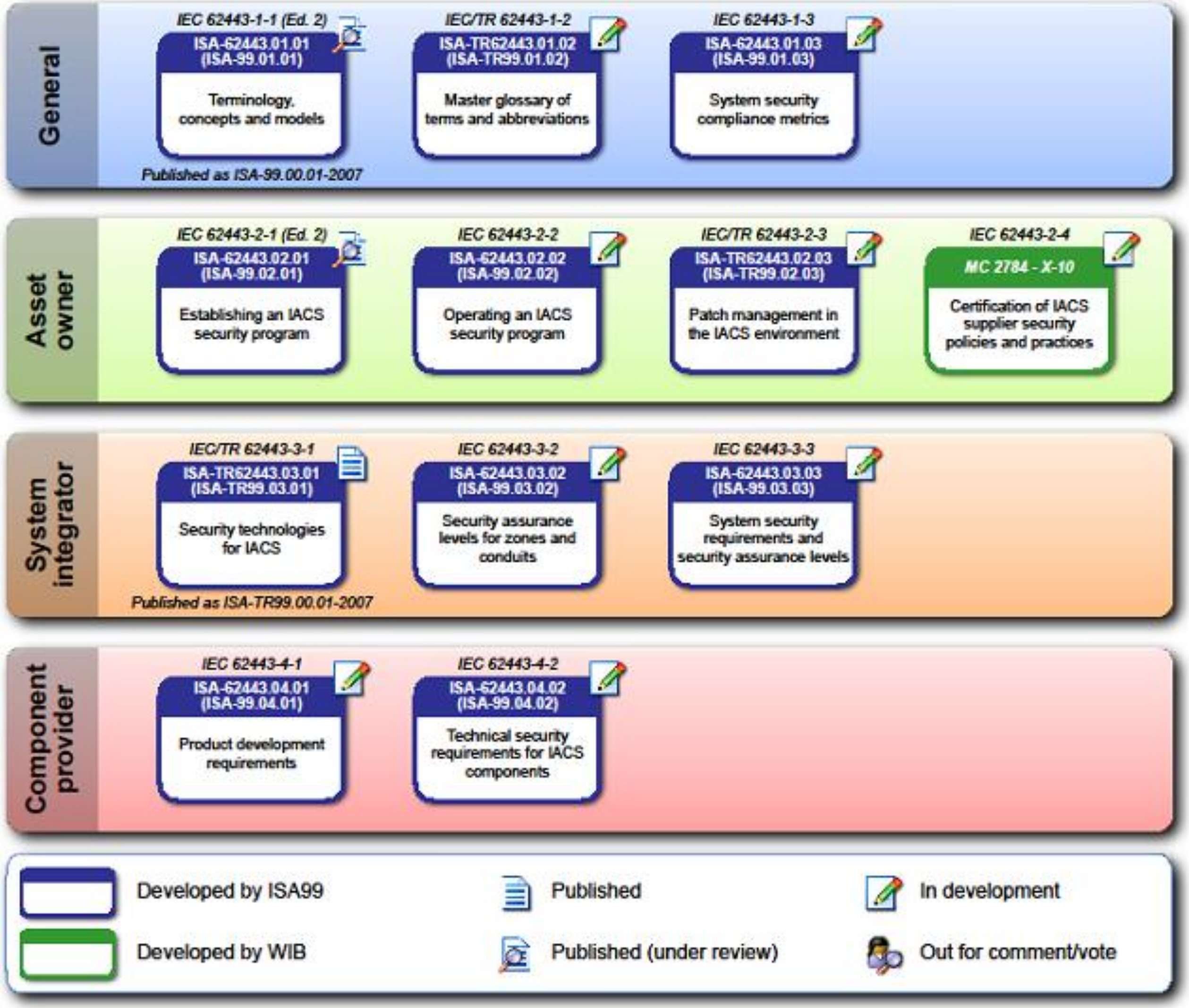


ISA (ISA99) Standards

- Manufacturing and control systems electronic security applied in the broadest possible sense is addressed
- Encompasses all types of plants, facilities and systems throughout all industries
- The recent emergence of malware such as Stuxnet has heightened the awareness of vulnerabilities in control systems



ISA99 Standards



General

- IEC 62443-1-1 (Ed. 2) – ISA-62443.01.01 (ISA-99.01.01) – Terminology, concepts and models
- IEC/TR 62443-1-2 – ISA-TR62443.01.02 (ISA-TR99.01.02) – Master glossary of terms and abbreviations
- IEC 62443-1-3 – ISA-62443.01.03 (ISA-99.01.03) – System security compliance metrics

Published as ISA-99.00.01-2007

Asset owner

- IEC 62443-2-1 (Ed. 2) – ISA-62443.02.01 (ISA-99.02.01) – Establishing an IACS security program
- IEC 62443-2-2 – ISA-62443.02.02 (ISA-99.02.02) – Operating an IACS security program
- IEC/TR 62443-2-3 – ISA-TR62443.02.03 (ISA-TR99.02.03) – Patch management in the IACS environment
- IEC 62443-2-4 – MC 2784 - X-10 – Certification of IACS supplier security policies and practices

System integrator

- IEC/TR 62443-3-1 – ISA-TR62443.03.01 (ISA-TR99.03.01) – Security technologies for IACS
- IEC 62443-3-2 – ISA-62443.03.02 (ISA-99.03.02) – Security assurance levels for zones and conduits
- IEC 62443-3-3 – ISA-62443.03.03 (ISA-99.03.03) – System security requirements and security assurance levels

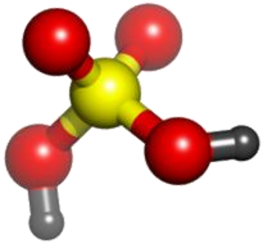
Published as ISA-TR99.00.01-2007

Component provider

- IEC 62443-4-1 – ISA-62443.04.01 (ISA-99.04.01) – Product development requirements
- IEC 62443-4-2 – ISA-62443.04.02 (ISA-99.04.02) – Technical security requirements for IACS components

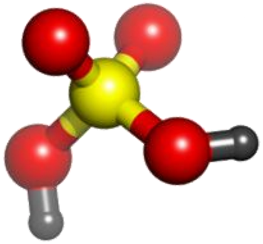
Developed by ISA99	Published	In development
Developed by WIB	Published (under review)	Out for comment/vote

http://upload.wikimedia.org/wikipedia/commons/1/1f/ISA99_Standards_Work_Products_2011.png



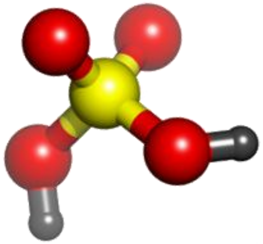
ISA99 Standards

- Manufacturing and control systems include, but are not limited to:
  - Hardware and software systems such as DCS (distributed control systems), PLC (programmable logic controllers) and SCADA (supervisory control and data acquisition), networked electronic sensing and monitoring/diagnostic systems
  - Human, network or machine interfaces to provide control to manufacturing operations in continuous, batch, discrete and other processes



ISA99 Standards

- Organized along four general categories:
  - Common concepts, models and terminology
  - Asset owners, addressing creation and maintenance of an effective industrial automation control system
  - System integrators
  - Component providers or vendors



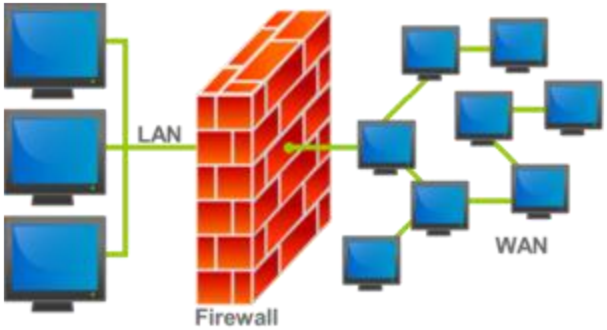
ISA Standards References

- http://www.isa.org/isa99
- http://www.isasecure.org

http://www.isa.org/Template.cfm?Section=Standards2

Best Practices for the Prevention of Cyber Attacks

- Cyber protection may be categorized as physical, administrative, and technical



http://upload.wikimedia.org/wikipedia/commons/thumb/5/5b/Firewall.png/300px-Firewall.png

http://monitorprivacyfilters.com/images/uploads/computer%20privacy%20screen.jpg

http://2.bp.blogspot.com/-g3AnydipNvM/T6P7tgj2spI/AAAAAAAAAk4/5ZL5aYCwFM0/s1600/Strong+Password+by+Marks+PC+Solution.webp

Best Practices for the Prevention of Cyber Attacks

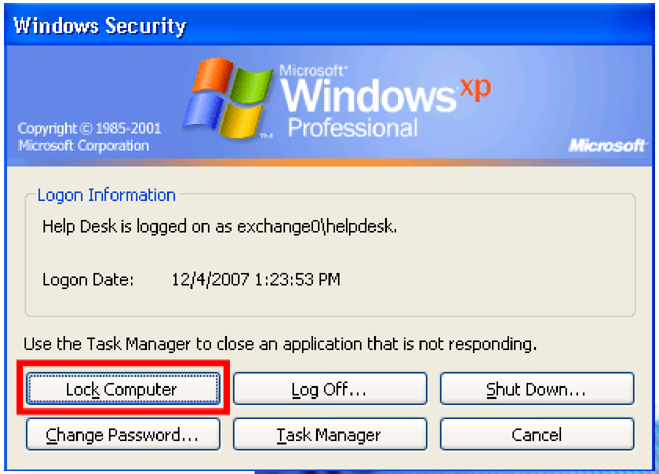
- Physical means
  - Barriers
    - Under direct physical control
    - Located in a building/room that is secure during non-operational hours
    - Blackout screens
  - Positioning
    - Only people with Need-to-Know (NTK) can view the screen

http://trustypony.com/wp-content/uploads/2007/12/laptop-privacy-screen.jpg

Best Practices for the Prevention of Cyber Attacks

- Administrative
  - Use of passwords and screen locks
  - Computer registration within system network
  - Appropriate markings (such as a barcode or unique sticker) on approved computers
  - Requiring physical or technical barriers

http://www2.le.ac.uk/offices/ias/images/lock-computer.gif


Windows Security

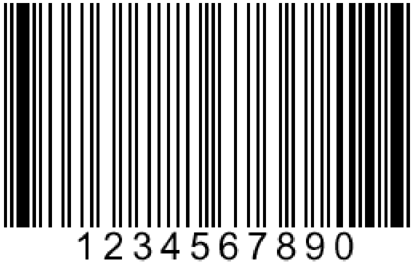
Logon Information

Help Desk is logged on as exchange0\helpdesk.

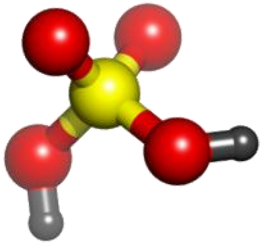
Logon Date: 12/4/2007 1:23:53 PM

Use the Task Manager to close an application that is not responding.

http://www.pps.k12.or.us/files/information-technology/password.jpg

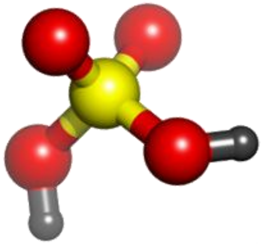


http://www.barcoding.com/images/Barcodes/code93.gif



Best Practices for the Prevention of Cyber Attacks

- Technical
  - Ensure all computers have antivirus software installed and is updated as necessary
  - Firewall protection ensures separation between internal networks and the external world
    - Prevents unauthorized external users from gaining access
    - Log session details between environments
    - Block programs and network traffic which could compromise systems
  - Use of Honeypot to learn more about attackers' interest to better prevent their future success



Best Practices for the Prevention of Cyber Attacks

- Minimal protection measures
  - Approved operating systems
  - Defined/managed configurations of software and operating systems
  - Protected or encrypted channels
  - Current antivirus protection
  - Firewalls
  - Adequate physical security
  - Registration with internal system
  - Authorized computer accounts
  - Password protected screen-locks

Information Recovery

- Secure connection to the internet (i.e., modem) to prevent infiltration
- Back-up information in multiple places
  - DVD
  - External hard drive
  - Server
- Recovery
  - Repair damaged systems or replace with new equipment
  - Reload operating system and software from master copies
  - Recover work from backups
  - Periodically test backup systems

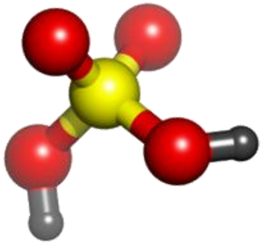
http://www.integratech.co.uk/uploads/1/5/154828.jpg

Information Disposal

- Maintain custody of electronic media
- Physically destroy items such as hard drives, thumb drives, CD, DVD

http://11k2.files.wordpress.com/2009/10/091017cd_shredder.jpg

http://static.guim.co.uk/sys-images/Technology/Pix/pictures/2009/1/8/1231425249253/Hard-Drive-Disposal-001.jpg



Case Study

Nuclear Power Station, USA (January 25, 2003)

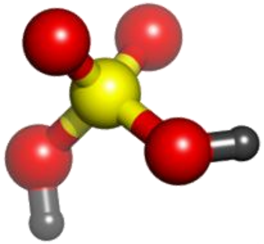
- Slammer worm began exploiting vulnerability Microsoft SQL server
  - No malicious payload, but caused a huge volume of spurious traffic
  - Traffic consumed bandwidth and clogged networks rendering them inaccessible
- Traveled from a consultant’s network to the corporate network
- Four hours, fifty minutes: Safety Parameter Display System (SPDS) could not be accessed
  - SPDS provides sensitive data about the reactor core (e.g., coolant systems, temperature sensors, radiation detectors)
  - These components are critical in identifying meltdown conditions and for response purposes
- Process control systems are vulnerable even if they are not connected to the internet
- Disrupted services outside of Power Station such as emergency response, airlines, and banking

Case Study

Worcester Airport, Massachusetts USA
(March 1997)

- Juvenile recreationally hacked into the telephone system that services Worcester, Massachusetts
- Attack shutdown telephone service to 600 customers in the community
- Disrupted local police and fire response and the local airport tower
- Airport tower correspondence disrupted for six hours
- Case displays the vulnerability of transportation, emergency response, and telecommunications

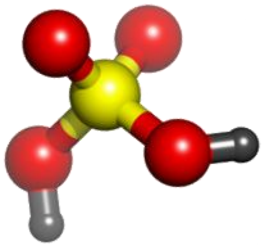
http://i.usatoday.net/community manager/_photos/today-in-the-sky/airports/jfk/tarmac-delayx-large.jpg



Case Study

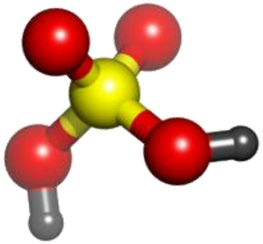
Maroochy Shire Council Sewage Release, Queensland, Australia (March – April 2000)

- Australian firm Hunter Watertech installed SCADA radio-controlled sewage equipment for Maroochy Shire Council
- Installer walked away from a strained relationship with Hunter Watertech; applied and denied a position at Maroochy Shire Council
- Decided to get revenge on both companies
- Attacker used laptop, two-way radios identical to the ones used by the Council, computer control device to systematically infiltrate and sabotage the sewage system



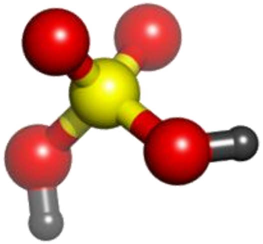
Case Study

- At least 46 occasions, former employee issued radio commands to the sewage equipment
  - Caused 800,000 liters of raw sewage to spill out into local parks and rivers
  - Marine life died, creek water turned black, stench was unbearable for residents
- Attacker had intimate knowledge of the control system technology
  - Ability to disguise actions
  - Difficultly in determining that attacks were intentional as opposed to malfunctions
- Contractor did not have adequate management, technical, and operational controls
- No existing cyber security policies or defenses were in place
- Classic example of insider threat resulting in severe exploitation

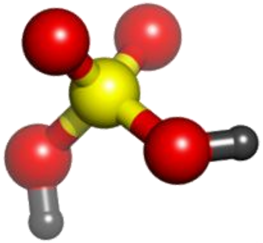


Section Summary

- Common definitions for terms used in cyber security
- Impact of cyber security as a growing threat to various industries of all size and missions
- Types of cyber attacks by various contributing parties (including motivations)
- Cyber security standards and guidance documents
- Best practices in cyber protection methods
- Information recovery
- Case studies



Questions?



Security Vulnerability Assessment

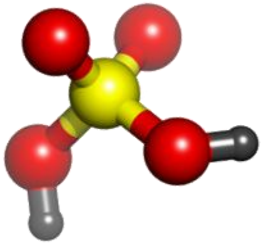
Table Top Exercise

SAND No. 2012-2012-4001 C , 2012-4378 P
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

CSP CHEMICAL SECURITY ENGAGEMENT PROGRAM

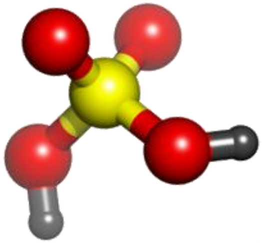
SAND 2012-5234C

Sandia National Laboratories



Terminology

- Turnstile = باب دوار
- Barrier = حاجز
- Video = فيديو
- Locks = أقفال
- Sensors = الاستشعار
- Alarm control display =التنبيه مراقبة العرض
- Fence improvement =سياج تحسن
- Badge Reader PIN = شارة قارئPIN



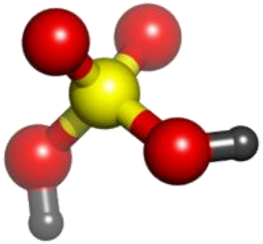
Investigating Safety & Security Incidents

SAND No. 2011-1036C
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000

CSP
CHEMICAL SECURITY
ENGAGEMENT PROGRAM

SAND 2012-5234C

Sandia National Laboratories



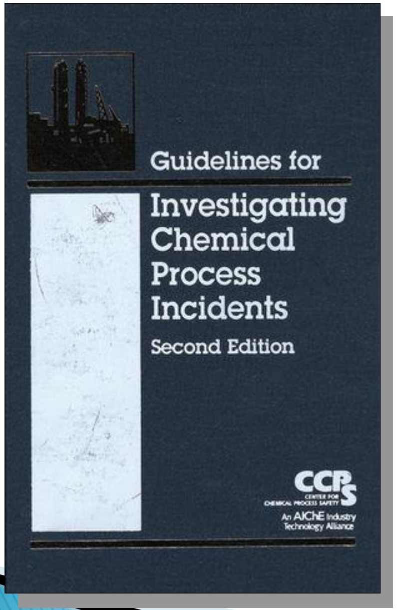
Key acronyms

RCA = *root cause analysis*

SVA = *security vulnerability analysis*

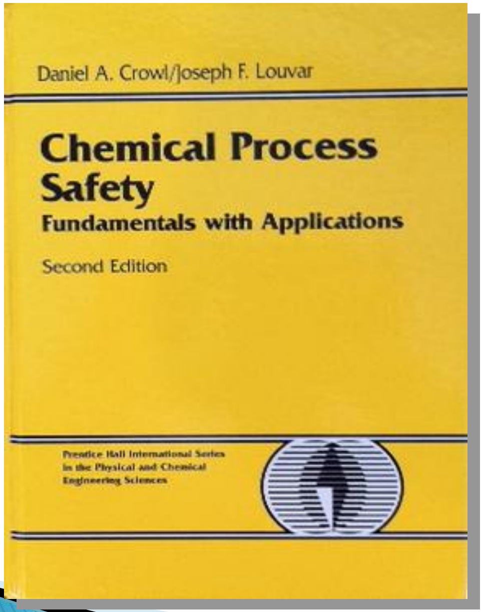
Resources

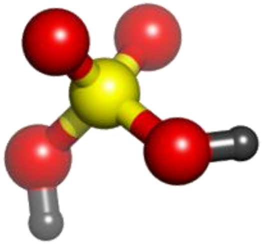
CCPS 2003. Center for Chemical Process Safety, *Guidelines for Investigating Chemical Process Incidents, 2nd Edition*, NY: AIChE.


Guidelines for
Investigating
Chemical
Process
Incidents
Second Edition
CCPS
CENTER FOR CHEMICAL PROCESS SAFETY
An AIChE Industry Technology Alliance

Resources

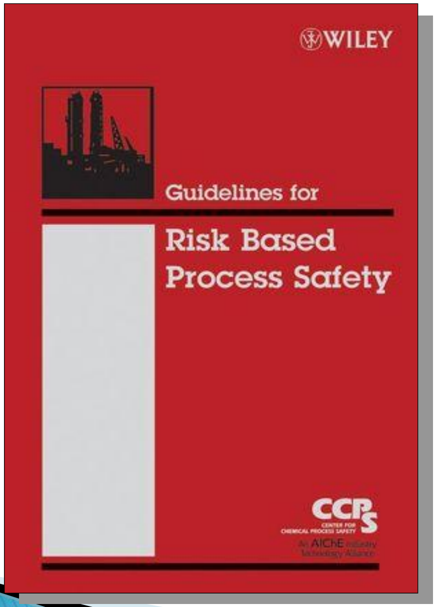
D.A. Crowl and J.F. Louvar 2001. *Chemical Process Safety: Fundamentals with Applications, 2nd Ed.*, Upper Saddle River, NJ: Prentice Hall.


Daniel A. Crowl/Joseph F. Louvar
Chemical Process Safety
Fundamentals with Applications
Second Edition
Prentice Hall International Series in the Physical and Chemical Engineering Sciences



Resources

CCPS 2007a. Center for Chemical Process Safety, *Guidelines for Risk Based Process Safety*, NY: AIChE.



WILEY

Guidelines for

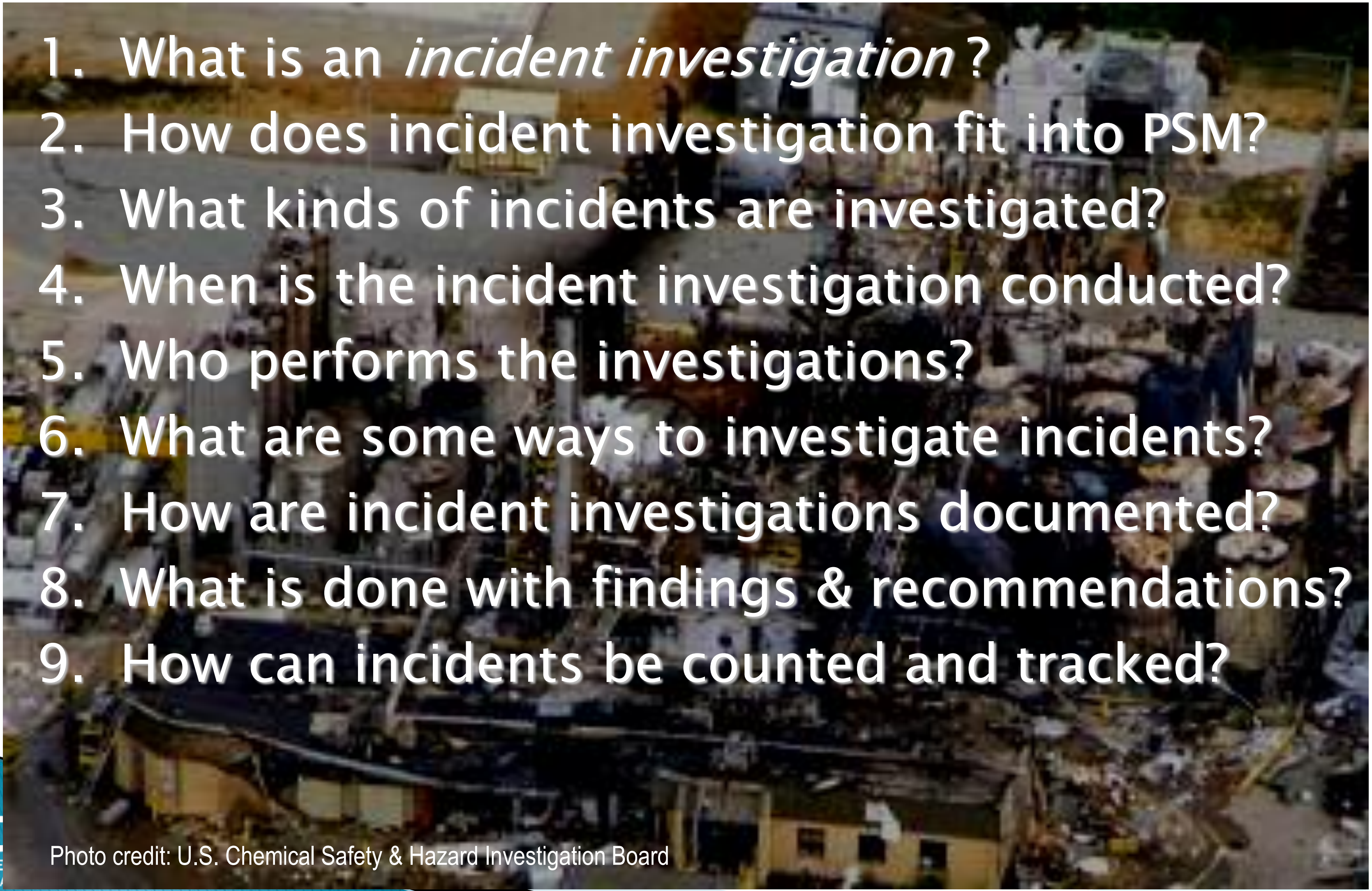
Risk Based Process Safety

CCPS

CENTER FOR CHEMICAL PROCESS SAFETY

An AIChE Industry Technology Alliance

Investigating Safety/Security Incidents



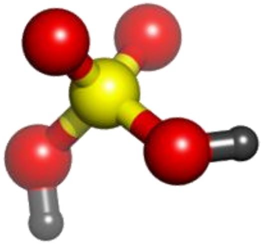
1. What is an *incident investigation* ?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. How are incident investigations documented?
8. What is done with findings & recommendations?
9. How can incidents be counted and tracked?

Photo credit: U.S. Chemical Safety & Hazard Investigation Board

Investigating Safety/Security Incidents

1. What is an *incident investigation*?

Results of explosion and fire at a waste flammable solvent processing facility
(U.S. CSB Case Study 2009-10-I-OH)



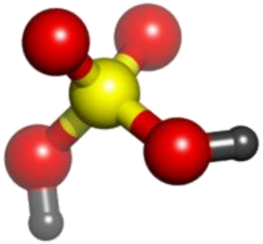
What is an *incident investigation*?

An *incident investigation*
is the management process

by which underlying causes of
undesirable events are uncovered

and steps are taken to
prevent similar occurrences.

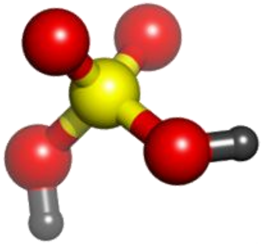
– CCPS 2003



Learning from incidents

Investigations that will enhance learning

- are fact-finding, not fault-finding
- must get to the *root causes*
- must be reported, shared and retained.



Definition – Root cause

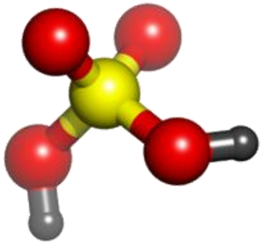
Root Cause: A fundamental, underlying, system-related reason why an incident occurred that identifies a correctable failure or failures in management systems.

There is typically more than one root cause for every process safety incident.

– CCPS 2003

Investigating Safety/Security Incidents

1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?



What kinds of incidents are investigated?

- The first step in an incident investigation is ***recognizing that an "incident" has occurred!***

What kinds of incidents are investigated?

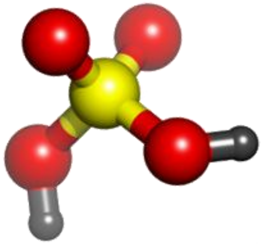
- The first step in an incident investigation is *recognizing that an "incident" has occurred!*

Yes

What kinds of incidents are investigated?

- The first step in an incident investigation is *recognizing that an "incident" has occurred!*

?

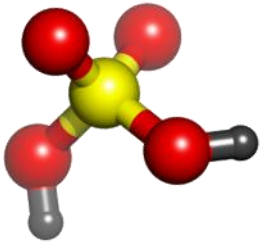


Definitions

Incident: An unplanned event or sequence of events that either resulted in or had the potential to result in adverse impacts.

Incident sequence: A series of events composed of an initiating cause and intermediate events leading to an undesirable outcome.

Source: CCPS 2008a



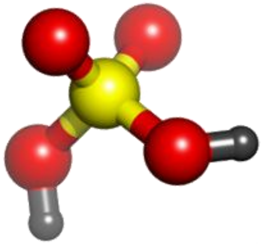
Incident types

Three categories of **incidents**, based on outcomes:

Loss event

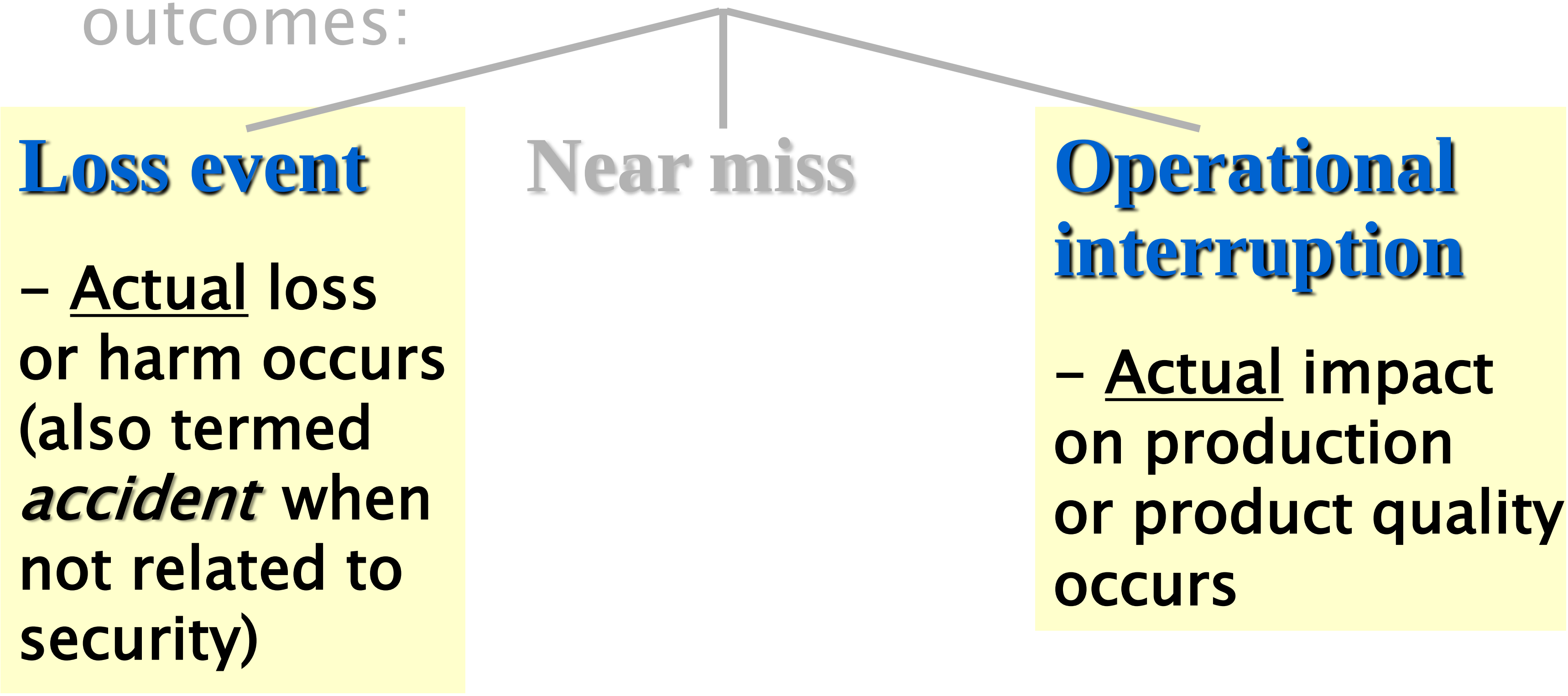
Near miss

Operational interruption



Incident types

Three categories of **incidents**, based on outcomes:



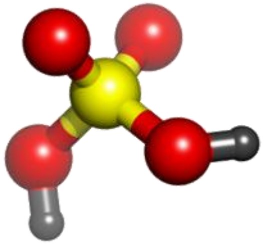
Loss event

– Actual loss or harm occurs (also termed *accident* when not related to security)

Near miss

Operational interruption

– Actual impact on production or product quality occurs



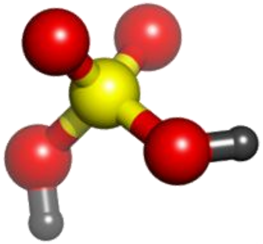
Incident types

Three categories of **incidents**, based on outcomes:

Loss event
Near miss
Operational interruption

Near miss: **An occurrence in which an accident (i.e., property damage, environmental impact, or human loss) or an operational interruption could have plausibly resulted if circumstances had been slightly different.**

- CCPS 2003



DISCUSSION

Give three or four examples of simple near-miss scenarios.

Include at least one related to facility security.

1.

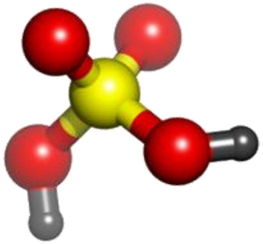
2.

3.

4.

Investigating Safety/Security Incidents

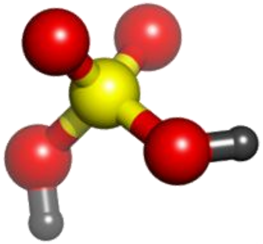
1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. **When is the incident investigation conducted?**



When is the incident investigation conducted?

- Basic answer: *As soon as possible.*
- Reasons:
  - Evidence gets lost or modified
    - Computer control historical data overwritten
    - Outside scene exposed to rain, wind, sunlight
    - Chemical residues oxidize, etc.
  - Witness memories fade or change
  - Other incidents may be avoided
  - Restart may depend on completing actions to prevent recurrence
  - Regulators or others may require it

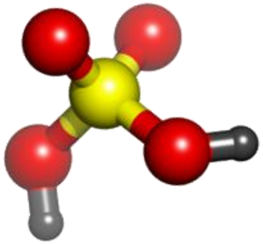
    (E.g., U.S. OSHA PSM: Start within 48 h)



When is the incident investigation conducted?

Challenges to starting as soon as possible:

- Team must be selected and assembled
- Team may need to be trained
- Team may need to be equipped
- Team members may need to travel to site
- Authorities or others may block access
- Site may be unsafe to approach / enter



DISCUSSION

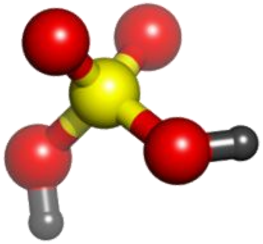
What might be done to overcome some of the challenges to starting an investigation?

○

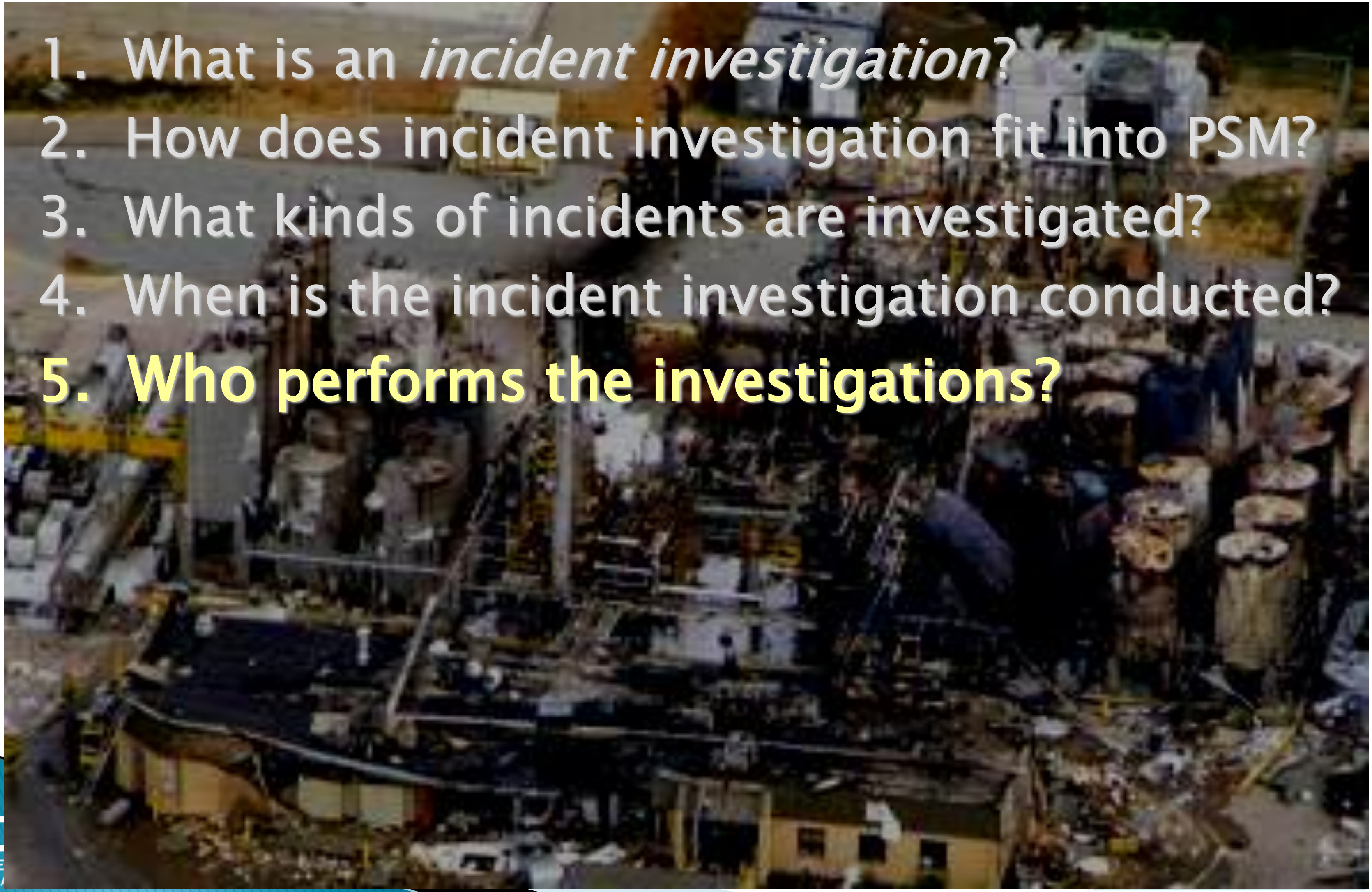
○

○

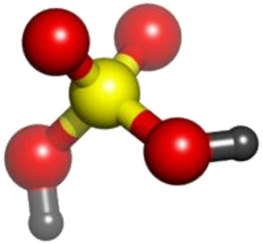
○



Investigating Safety/Security Incidents



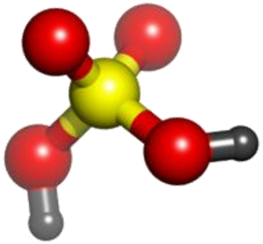
1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. **Who performs the investigations?**



Who performs the investigations?

Options:

- Single investigator
- Team approach



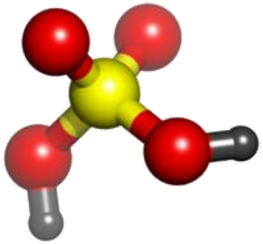
Who performs the investigations?

Options:

- Single investigator
- Team approach

Advantages of team approach: (CCPS 2003)

- Multiple technical perspectives help analyze findings
- Diverse personal viewpoints enhance objectivity
- Internal peer reviews can enhance quality
- More resources are available to do required tasks
- Regulatory authority may require it



Who performs the investigations?

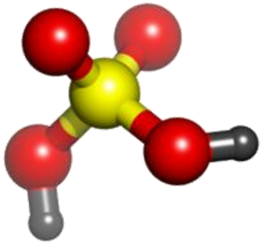
The “best team” will vary depending on the nature, severity and complexity of the incident.

Some possible team members:

- Team leader / investigation method facilitator
- Area operator
- Process engineer
- Safety/security specialist
- I&E / process control or computer systems support
- Union safety representative
- Contractor representative
- Other specialists (e.g., metallurgist, chemist)

Investigating Safety/Security Incidents

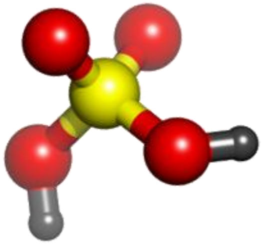
1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. **What are some ways to investigate incidents?**



Older investigations

- Only identified obvious causes; e.g.,
  - “The line plugged up”
  - “The operator messed up”
  - “The whole thing just blew up”

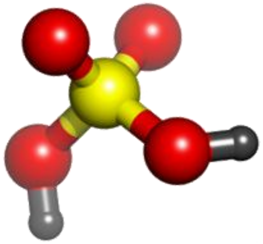
- Recommendations were superficial
  - “Clean out the plugged line”
  - “Re-train the operator”
  - “Build a new one”



Layered investigations

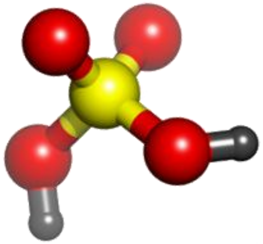
- Deeper analysis
- Additional layers of recommendations:

1. Immediate technical recommendations
   - *e.g., replace the carbon steel with stainless steel*
2. Recommendations to avoid the hazards
   - *e.g., use a noncorrosive process material*
3. Recommendations to improve the management system
   - *e.g., keep a materials expert on staff*



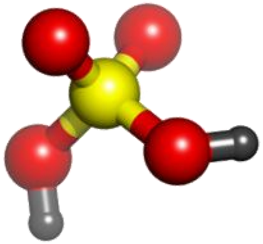
Case Study

- Pool is very crowded
- Older children are engaged in “horseplay”
- 5 year old child pushed into deep end of pool
- Lifeguard does not notice child in deep end



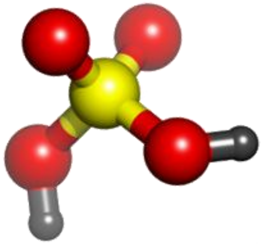
Technical Recommendations

- Paint pool to indicated deep end
- Add more lifeguards
- Reduce number of swimmers



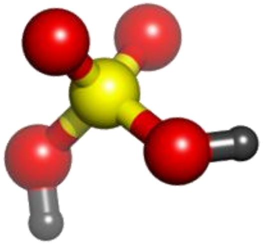
Avoiding the Hazard

- Zone the pool–young children at one end of the pool
- Swimming lessons
- All new swimmers get pool orientation
- Add another roving lifeguard



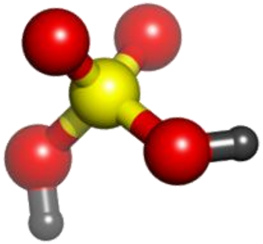
Improve the Management System

- Train lifeguards to alert supervision of potential problems
- Assign a supervisor to make formal inspections on a regular basis



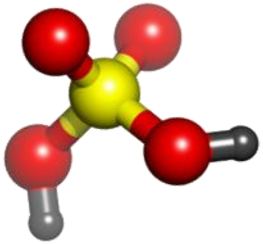
Investigation process

1. Choose investigation team
2. Make brief overview survey
3. Set objectives, delegate responsibilities
4. Gather, organize pre-incident facts
5. Investigate, record incident facts
6. Research, analyze unknowns
7. Discuss, conclude, recommend
8. Write clear, concise, accurate report



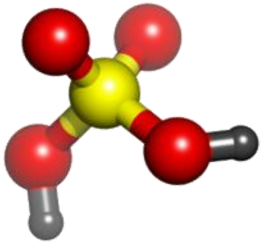
Discovery phase

- Develop a plan
- Gather evidence
  - Take safety precautions; use PPE
  - Preserve the physical scene and process data
  - Gather physical evidence, samples
  - Take photographs, videos
  - Interview witnesses
  - Obtain control or computer system charts and data



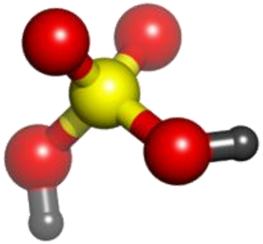
Analysis of facts

- Develop a timeline
- Analyze physical and/or electronic evidence
  - Chemical analysis
  - Mechanical testing
  - Computer modeling
  - Data logs
  - etc.
- Conduct multiple-root-cause analysis



Some analysis methods

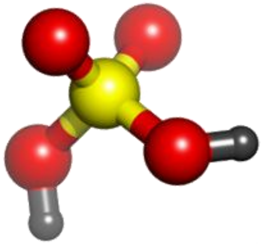
- Five Why's
- Causal Tree
- RCA (Root Cause Analysis)
- FTA (Fault Tree Analysis)
- MORT (Management Oversight and Risk Tree)
- MCSOII (Multiple Cause, Systems Oriented Incident Investigation)
- TapRooT®



Some analysis methods

General analysis approach:

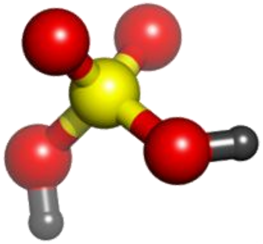
- Develop, by brainstorming or a more structured approach, possible **incident sequences**
- Eliminate as many incident sequences as possible based on the available evidence
- Take a closer look at those that remain until the actual incident sequence is discovered (if possible)
- Determine the underlying root causes of the actual incident sequence



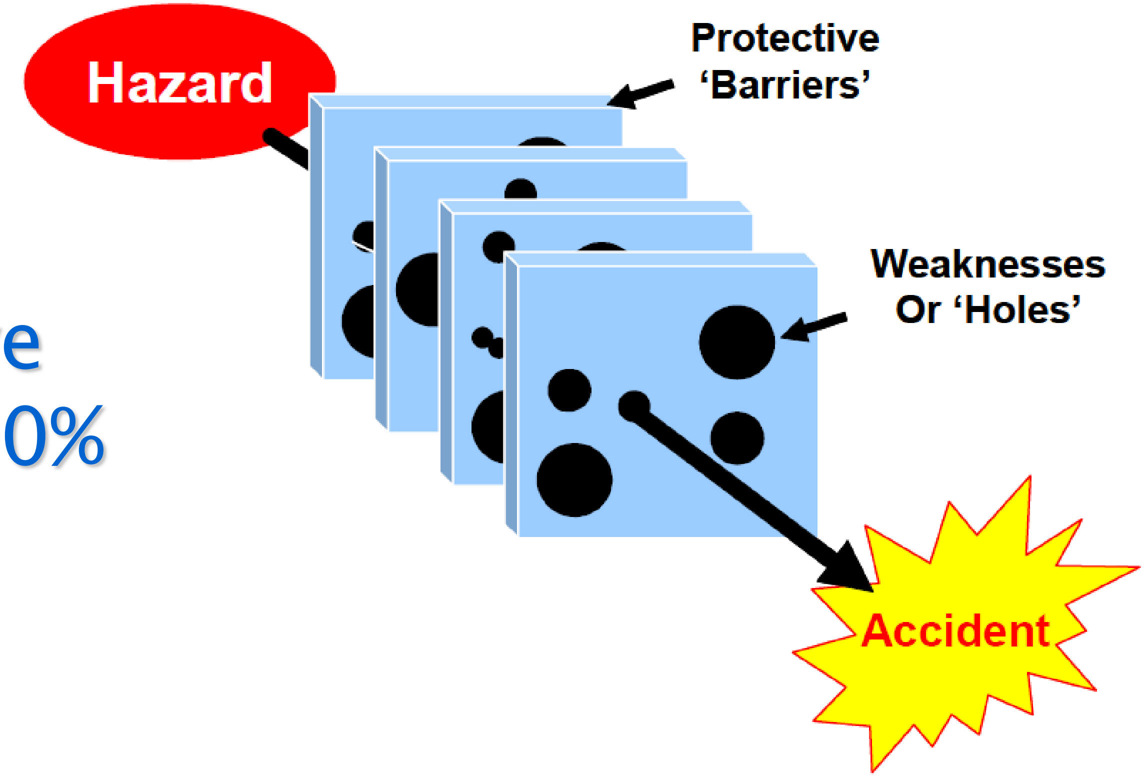
Incident sequence questions

Determine, for the incident being investigated:

- What was the *cause* or *attack* that changed the situation from “normal” to “abnormal”?
- What was the actual (or potential, if a near miss) *loss event*?
- What safeguards failed? What did not fail?

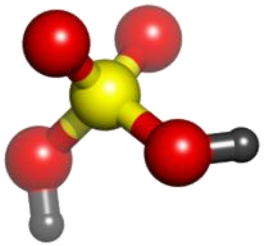


“Swiss cheese model” review



REMEMBER:

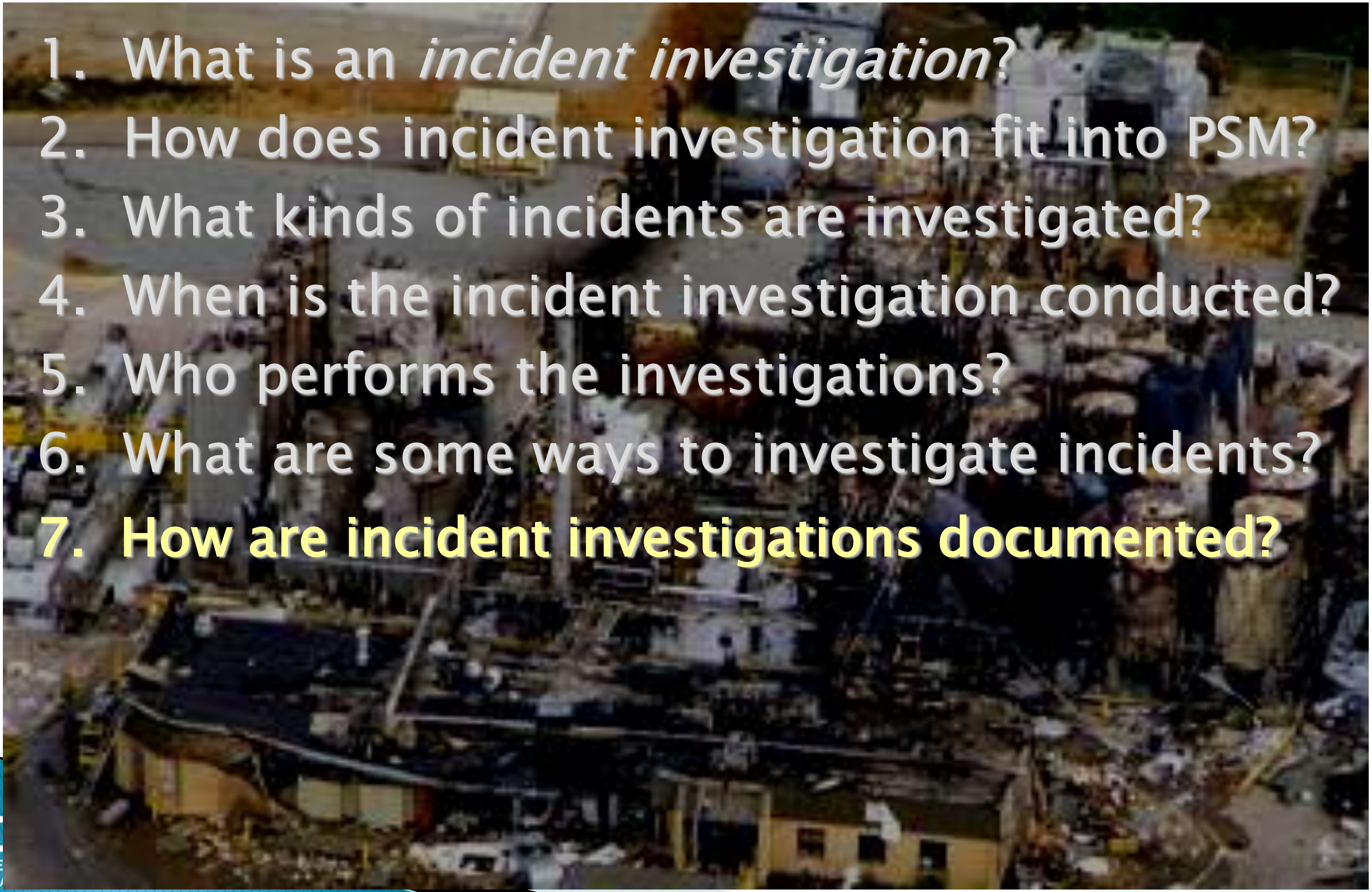
No protective barrier is 100% reliable.



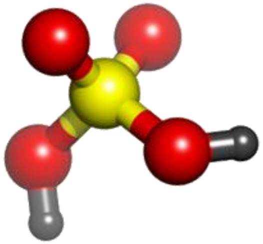
Discuss, conclude, recommend

- Find the most likely scenario that fits the facts
- Determine the underlying management system failures
- Develop layered recommendations

Investigating Safety/Security Incidents



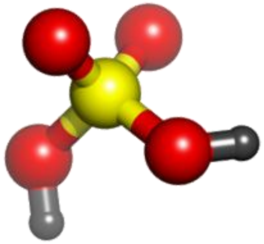
1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. **How are incident investigations documented?**



How are incident investigations documented?

A written report documents, as a minimum:

- Date of the incident
- When the investigation began
- Who conducted the investigation
- A description of the incident
- The factors that contributed to the incident
- Any recommendations resulting from the investigation



Typical report format

1 Introduction

2 System description

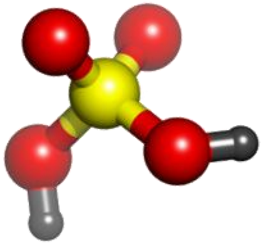
3 Incident description

4 Investigation results

5 Discussion

6 Conclusions

7 Layered recommendations

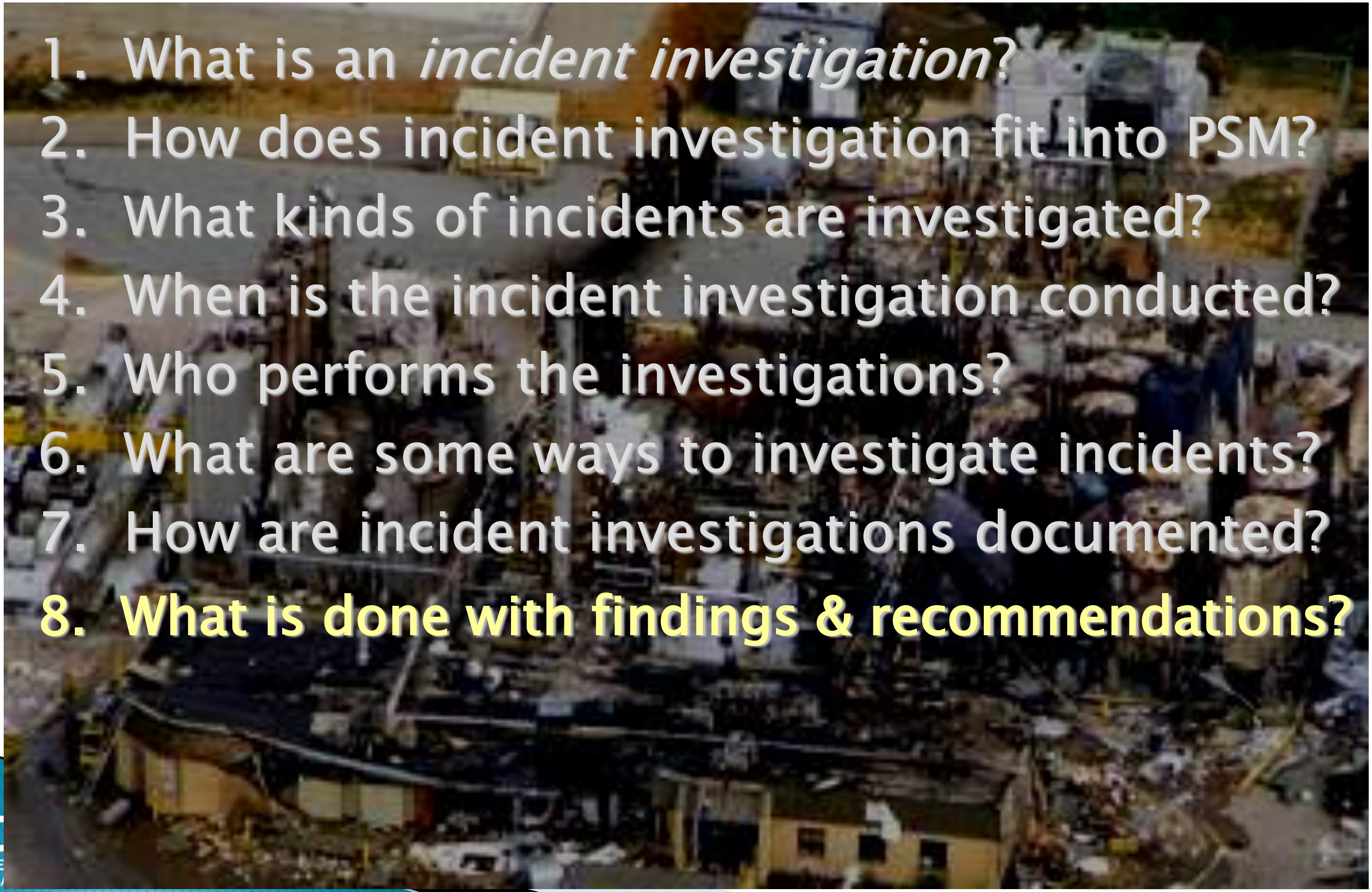


Investigation Summary

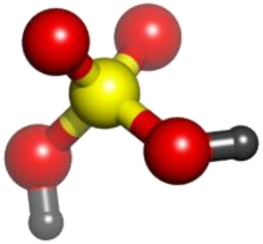
- The investigation report is generally too detailed to share the learnings to most interested persons

- An Investigation Summary can be used for broader dissemination, such as to:
  - Communicate to management
  - Use in safety or security meetings
  - Train new personnel
  - Share lessons learned with sister plants

Investigating Safety/Security Incidents



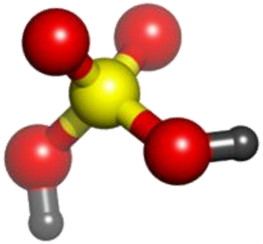
1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. How are incident investigations documented?
8. **What is done with findings & recommendations?**



Findings and recommendations

What is the most important product of an incident investigation?

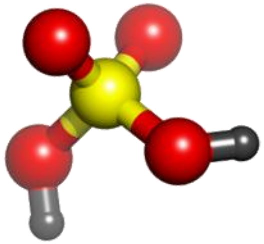
1. The incident report
2. Knowing who to blame for the incident
3. Findings and recommendations from the study



Findings and recommendations

What is the most important product of an incident investigation?

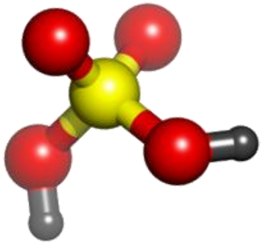
1. The incident report
2. Knowing who to blame for the incident
3. Findings and recommendations from the study
4. The actions taken in response to the study findings and recommendations



Findings and recommendations

Example form to document recommendations:

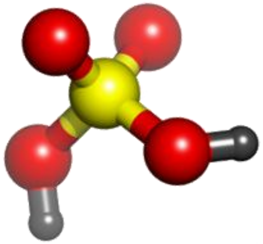
ORIGINAL STUDY FINDING / RECOMMENDATION			
Source:	□ PHA □ Incident Investigation □ Compliance Audit □ Self-Assessment □ Other		
Source Name			
Finding No.		**Risk-Based Priority** *(A, B, C or N/A)*	
Finding / Rec-ommendation			
Date of Study or Date Finding / Recommendation Made			



Aids for recommendations

Overriding principles (Crowl and Louvar 2001, p. 528):

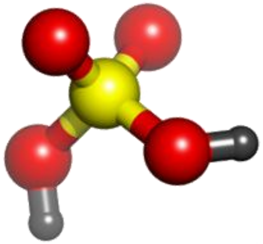
- Make safety [and security] investments on cost and performance basis
- Improve management systems
- Improve management and staff support
- Develop layered recommendations, especially to eliminate underlying causes



Aids for recommendations

Overriding principles:

- Make safety [and security] investments on cost and performance basis
- Improve management systems
- Improve management and staff support
- Develop layered recommendations, especially to eliminate underlying causes **and hazards**

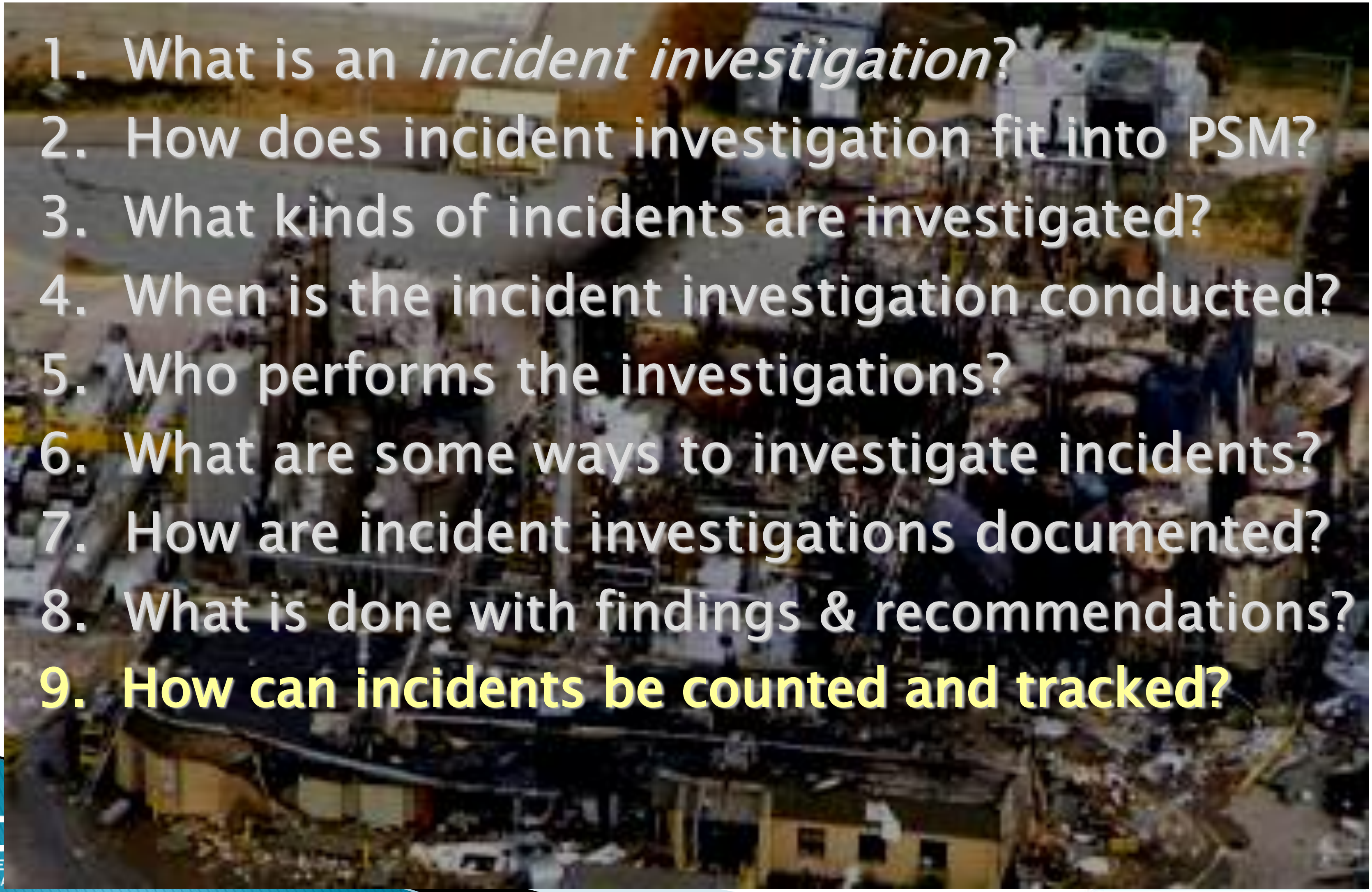


Implementation

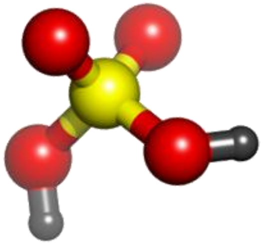
A system must be in place to ensure all incident investigation action items are completed on time and as intended.

- Same system can be used for both hazard analysis and incident investigation action items
- Include regular status reports to management
- Communicate actions to affected employees

Investigating Safety/Security Incidents



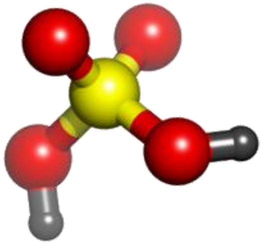
1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. How are incident investigations documented?
8. What is done with findings & recommendations?
9. How can incidents be counted and tracked?



How can incidents be counted and tracked?

"**Lagging indicators**" — *actual loss events*

- Major incident counts and monetary losses
- Injury/illness rates
- Process safety incident rates



How can incidents be counted and tracked?

"Lagging indicators" — *actual loss events*

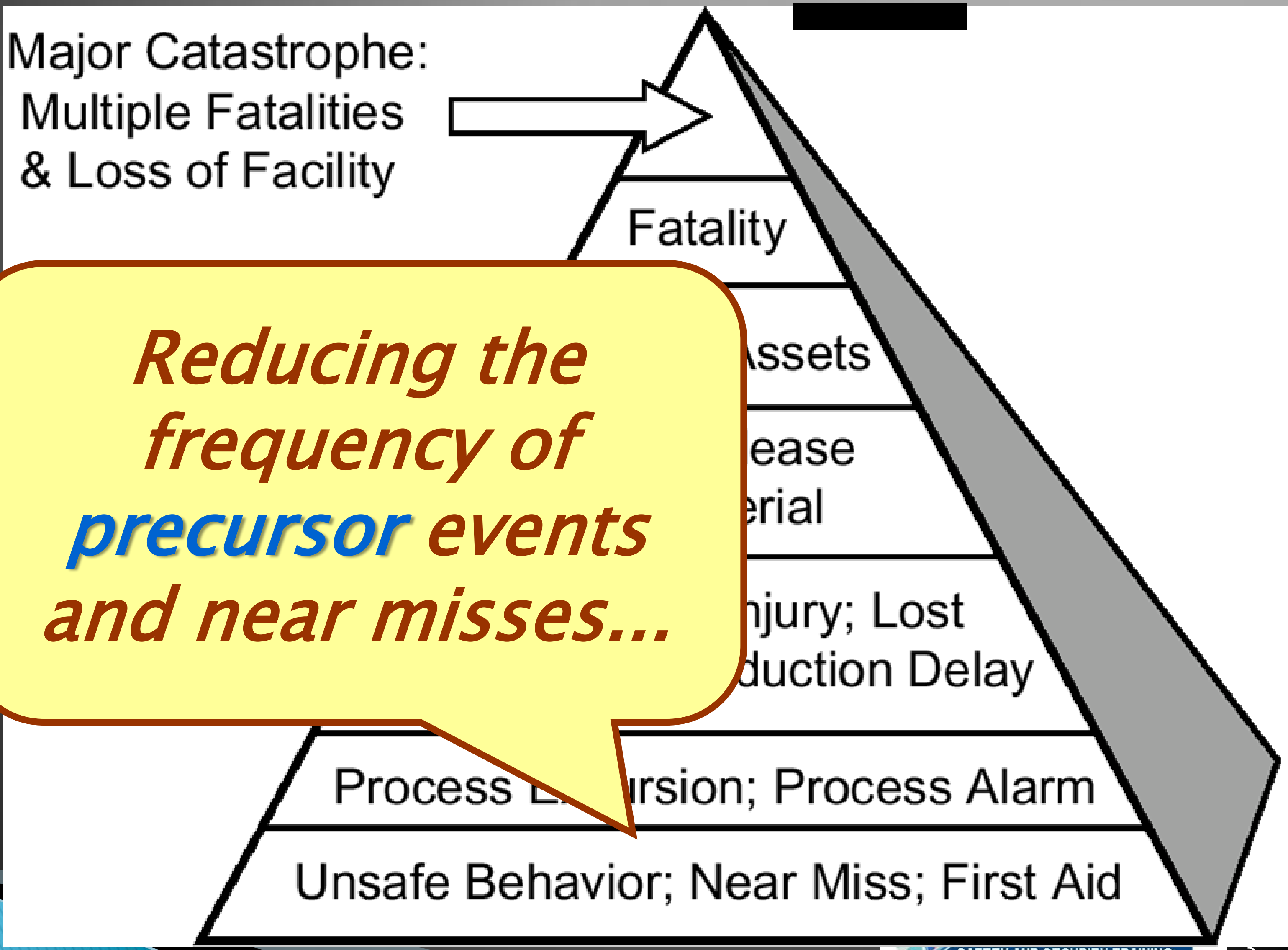
- Major incident counts and monetary losses
- Injury/illness rates
- Process safety incident rates

"Leading indicators" — *precursor events*

- Near misses
- Abnormal situations
  - E.g., Overpressure relief events
  - Safety alarm or shutdown system actuations
  - Flammable gas detector trips
- Unsafe acts and conditions
- Other PSM element metrics

Pyramid Principle

[redacted]



Major Catastrophe:
Multiple Fatalities
& Loss of Facility

Fatality

ssets

ease
erial

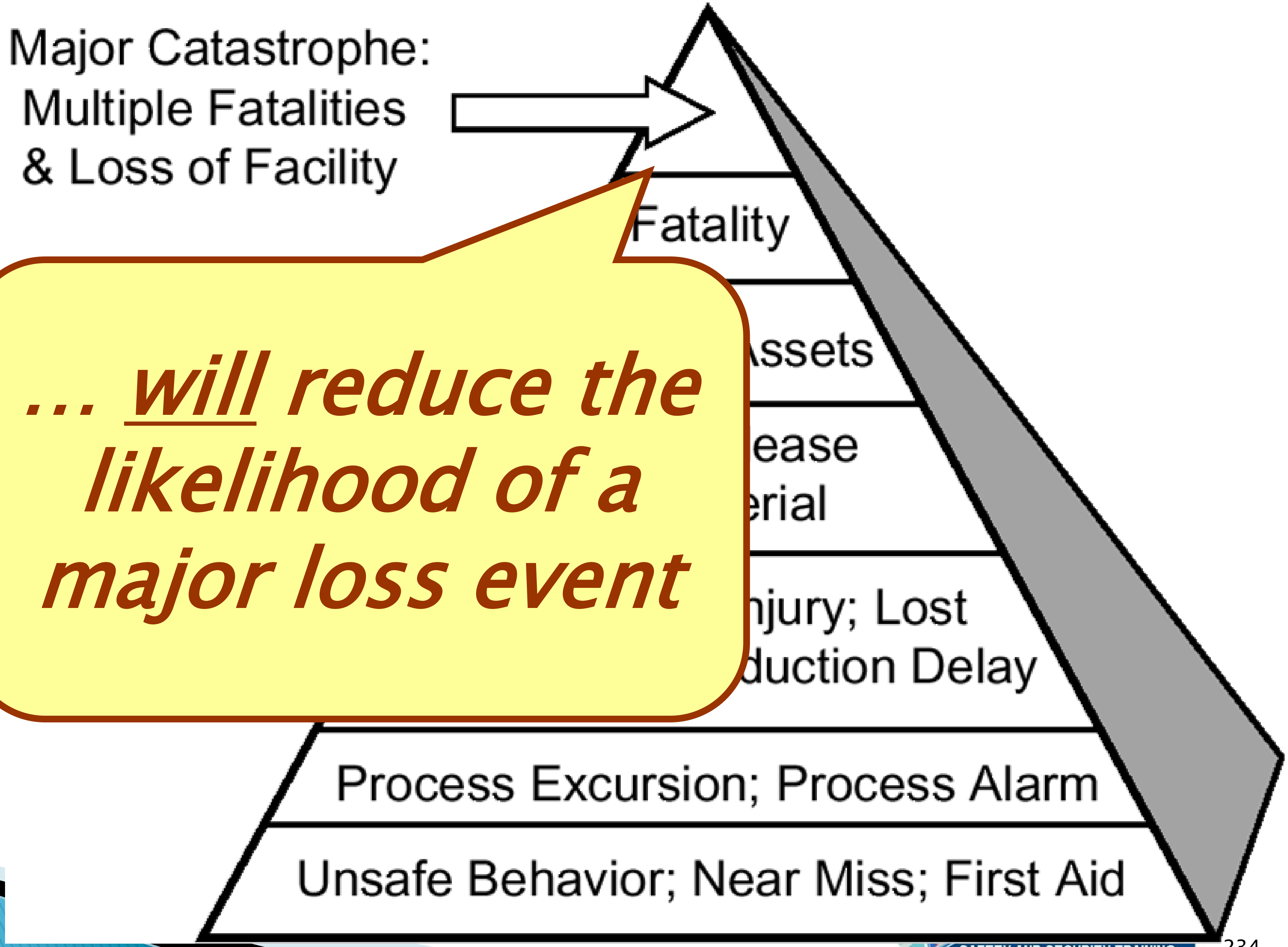
njury; Lost
duction Delay

Process E rsion; Process Alarm

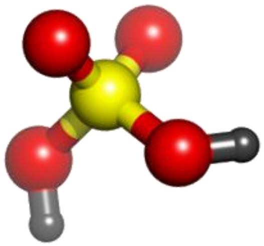
Unsafe Behavior; Near Miss; First Aid

*Reducing the frequency of **precursor** events and near misses…*

Pyramid Principle



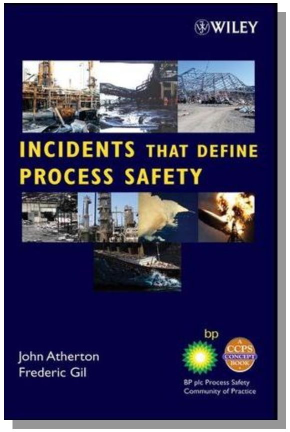
… will reduce the likelihood of a major loss event



Additional resources

- AIChE ***Loss Prevention Symposium***, Case Histories session (every year)
- www.csb.gov reports and videos
- CCPS 2008b, Center for Chemical Process Safety, ***Incidents that Define Process Safety***, NY: AIChE
- CCPS, "**Process safety leading and lagging metrics – You don't improve what you don't measure,**"

www.aiche.org/uploadedFiles/CCPS/Publications/CCPS_ProcessSafety2011_2-24.pdf



WILEY

INCIDENTS THAT DEFINE PROCESS SAFETY

John Atherton
Frederic Gil

bp

CCPS CONCEPT BOOK

BP plc Process Safety Community of Practice